УДК 681.391.837: 681.327.22

В.І. Барсов

Українська інженерно-педагогічна академія, Харків

РЕАЛІЗАЦІЯ МЕТОДУ ВИКОНАННЯ ОПЕРАЦІЇ ПІДНЕСЕННЯ ЧИСЕЛ ДО КВАДРАТУ ЗА ДОВІЛЬНИМ МОДУЛЕМ МСЧ

У даній статті розглянута технічна реалізація системи криптографічної обробки інформації на основі використання модулярної системи числення (МСЧ). Це дозволить зменшити обчислювальну складність реалізації процесу криптографічних перетворень, а також підвищити ефективність контролю й корекції помилок інформації.

Ключові слова: *система обробки криптографічної, криптографічні перетворення, модулярна система числення.*

Вступ

Характерним для сучасного технологічного застосування криптографічних технічних засобів, що реалізують криптографічні перетворення (КП) є істотне зростання вимог до швидкості обробки інформації при виконанні КП і надійності (відмовостійкості) їх функціонування. Під обчислювально-складними задачами криптографічних перетворень розуміють задачі, що заздалегідь мають рішення, але для його знаходження необхідно проведення надзвичайно великої кількості операцій обчислювача (універсальних ЕОМ або спеціалізованого процесора обробки криптографічної інформації (СОКІ)).

Існують два принципові шляхи зниження обчислювальної складності реалізації криптографічного алгоритму: часткове скорочення кількості операцій і зменшення часу реалізації кожної операції. Перший шлях припускає зміну (модифікацію) алгоритму, це вельми трудомісткий процес і навряд чи це доцільно і взагалі можливо. Другий шлях – базується на зменшенні часу виконання модульних операцій у криптоалгоритмі, які в сучасних СОКІ реалізуються у звичайній двійковій позиційній системі числення (ПСЧ).

У [2,4] показано, що криптографічні перетворення RSA практично складаються з двох основних типів модульних операцій: операції модульного множення і операцій піднесення чисел до квадрату за модулем m простого числа. Технічна реалізація даних операцій і складає основну обчислювальну складність криптографічних перетворень RSA. У відповідності з цим є актуальним проведення досліджень, які спрямовані на синтез пристроїв ефективної реалізації операції піднесення чисел до квадрату за модулем m_k простого числа.

Основна частина

У [2, 3] розглянуто синтез пристрою для реалізації операції піднесення чисел до квадрату за непарним модулем МСЧ. Тому у даній статті розглядається випадок реалізації операції піднесення чисел до квадрату за парним m_i модулем МСЧ.

При реалізації операції піднесення чисел до квадрата за парним m_i модулем МСЧ доцільно окремо розглянути два можливих варіанта: для $m_i/2$ парного та $m_i/2$ непарного чисел.

Функціонування пристрою, у відповідності до першого варіанту, визначається наступним математичним співвідношенням

$$\left(m_2 / 2\right)^2 = 0 \,(\mathrm{mod}\, m_2). \qquad (1)$$

Вираз (1) покладено в основу алгоритму для визначення значення $A^2(\mathrm{mod}\ m_2)$. В таблиці 2 представлено приклад алгоритму визначення $A^2(\mathrm{mod}\ m_2)$ для модуля $m_2 = 12$ ($m_2/2 = 6$).

Для другого варіанту реалізації операції піднесення чисел до квадрата за парним m_i модулем МСЧ ($m_3 = 2n$ парного та $m_3/2$ непарного чисел) виконується умова

$$\left(m_3/2\right)^2 \equiv \left(m_3 / 2\right) (\mathrm{mod}\, m_3). \qquad (2)$$

Дійсно, вираз (2) легко представити у вигляді

$$\frac{m_3}{2} \cdot \left(\frac{m_3}{2} - 1 \right) = 0 \,(\mathrm{mod}\, \frac{m_3}{2} \cdot 2). \qquad (3)$$

З теорії чисел відомо, що порівняння $A \equiv B \ (\mathrm{mod}\ m_i)$ двох чисел A и B за модулем m_i рівнозначно подільності числа A–B на модуль m_i. З виразу (3) випливає, що число $m_3 = \left(m_3 / 2\right) \cdot 2$ є дільник виразу $\left(m_3 / 2\right) \cdot \left(\left(m_3 / 2\right) - 1\right)$ Дійсно, перший співмножник $\left(m_3 / 2\right)$ добутку (3) ділиться на $\left(m_3 / 2\right)$, а другий $\left(m_3 / 2\right) - 1$ співмножник – ділиться на два, так як за умовою (другий варіант) значення $\left(m_3 / 2\right)$ непарне число. Таким чином, рівняння (3) дійсно справедливе.

Вираз (2) покладено в основу алгоритму для визначення значення $A^2(\mathrm{mod}\ m_3)$. У таблиці 3 наведено приклад алгоритму визначення значення A^2 $(\mathrm{mod}\ m_3)$ для модуля $m_3 = 14$ ($m_3/2 = 7$).

На рис. 1 приведена загальна схема пристрою для реалізації операції піднесення чисел до квадрата за довільними модулями m_i МСЧ, де: 1 – вхід пристрою; 2 – вхідний регістр; 3, 4 і 5 – перша, друга і третя групи елементів I; 6, 7 і 8 – шини подачі сигналів ознак відповідно першого m_1, другого m_2 і третього m_3 модулів МСЧ; 9, 10 і 11 – перший, другий і третій дешифратори (пристрій для перетворення числа з двійкового коду в унітарний); 12 – перша група двох входових елементів АБО; 13 – перший шифратор (пристрій для перетворення унітарного коду числа в двійковий); 14 - друга група двох входових елементів АБО; 15 - другий шифратор; 16 - третя група двох входових елементів АБО; 17 - третій шифратор; 18 – четверта група елементів АБО; 19 – вихідний регістр; 20 – вихід пристрою.

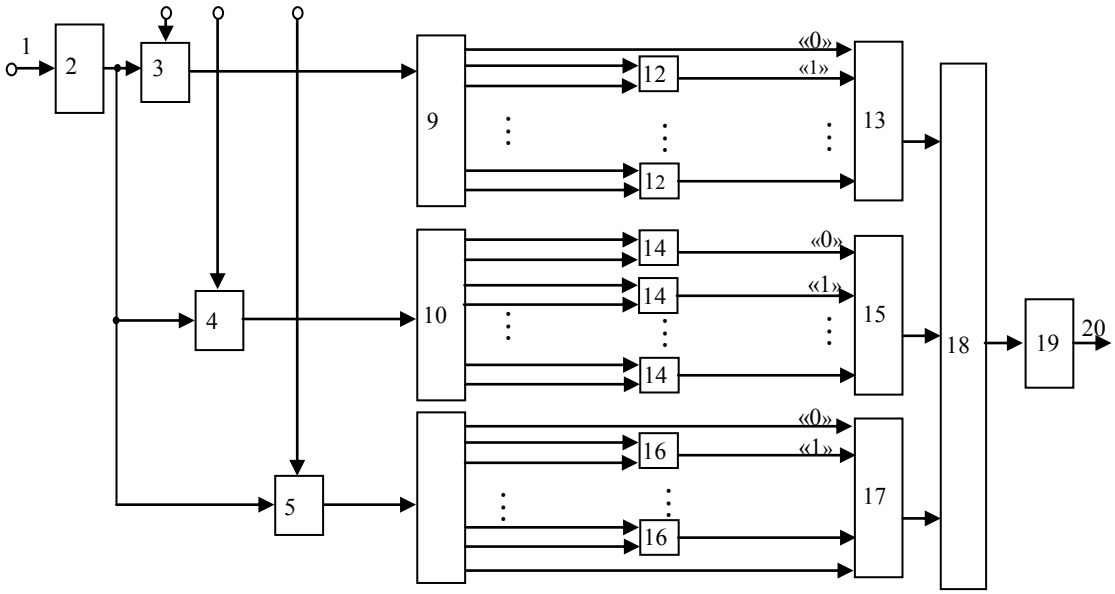

Рис. 1. Пристрій для реалізації операції піднесення чисел до квадрата за довільними модулями m_i МСЧ

Доцільно розглянути процес функціонування пристрою операції піднесення чисел до квадрату за модулем m простого числа у всіх трьох можливих режимах роботи. На рис. 2 приведено алгоритм реалізації операції піднесення чисел до квадрата за довільними модулями m_i МСЧ.

Перший режим. Якщо m_1 непарне число. Присутній сигнал шини 6.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I першої 3 групи число A $(0 \le A \le m_1 - 1)$ у двійковому коді поступає на вхід першого дешифратора 9 Дешифратор 9 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО першої 12 групи поступає на відповідний вхід першого 13 шифратора. Номери входів шифратора 13 відповідають значенням: 0, 1, 2^2 (mod m), 3^2 (mod m), 4^2 (mod m), …, $\left(\left[m / 2\right]\right)^2$ (mod m). З виходу шифратора 13 результат операції $A^2(\mathrm{mod}\, m_1)$ в двійковому коді через чет-

верту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою.

Другий режим (перший варіант реалізації операції піднесення чисел до квадрата за парним m_i модулем МСЧ). Якщо m_2 парне число. Присутній сигнал шини 7.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I другої 4 групи число A $(0 \le A \le m_2 - 1)$ у двійковому коді поступає на вхід другого дешифратора 10. Дешифратор 10 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО другої 14 групи поступає на відповідний вхід другого 15 шифратора. Номери входів шифратора 15 відповідають значенням $A^2(\mathrm{mod}\ m_2)$. З виходу шифратора 15 результат операції $A^2(\mathrm{mod}\, m_2)$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою.

Третій режим.(другий варіант реалізації операції піднесення чисел до квадрата за парним m_i модулем МСЧ). Якщо m_3 парне число. Присутній сигнал шини 8.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I третьої 5 групи число A $(0 \le A \le m_3 - 1)$ у двійковому коді поступає на вхід третього дешифратора 11 (фіг.2). Дешифратор 11 перетворює число A в унітарний код, сигнал якого через відповідний елемент АБО третьої 16 групи поступає на відповідний вхід третього 17 шифратора. Номери входів шифратора 13 відповідають значенням $A^2(\mathrm{mod}\ m_3)$. З виходу шифратора 17 результат операції $A^2(\mathrm{mod}\, m_3)$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою.

Розглянемо приклади конкретного виконання пристроєм операції $A^2(\mathrm{mod}\, m_i)$. *Перший режим*. При $m_1 = 11$ - непарне число, A = 8 (1000), (рис. 3, 4 і табл. 1). Присутній сигнал шини 6.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I першої 3 групи число A = 1000 у двійковому коді поступає на восьмий вхід першого дешифратора 9. Дешифратор 9 перетворює число A в унітарний код A = 8, сигнал якого через третій (табл. 4) елемент АБО першої 12 групи поступає на дев'ятий вхід першого 13 шифратора. З виходу шифратора 13 результат операції $A^2(\mathrm{mod}\, m_1) = 1001$ у двійковому коді через четверту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою. Перевірка: $A^2(\mathrm{mod}\ m_1) = 8^2(\mathrm{mod}\ 11) = 9$.

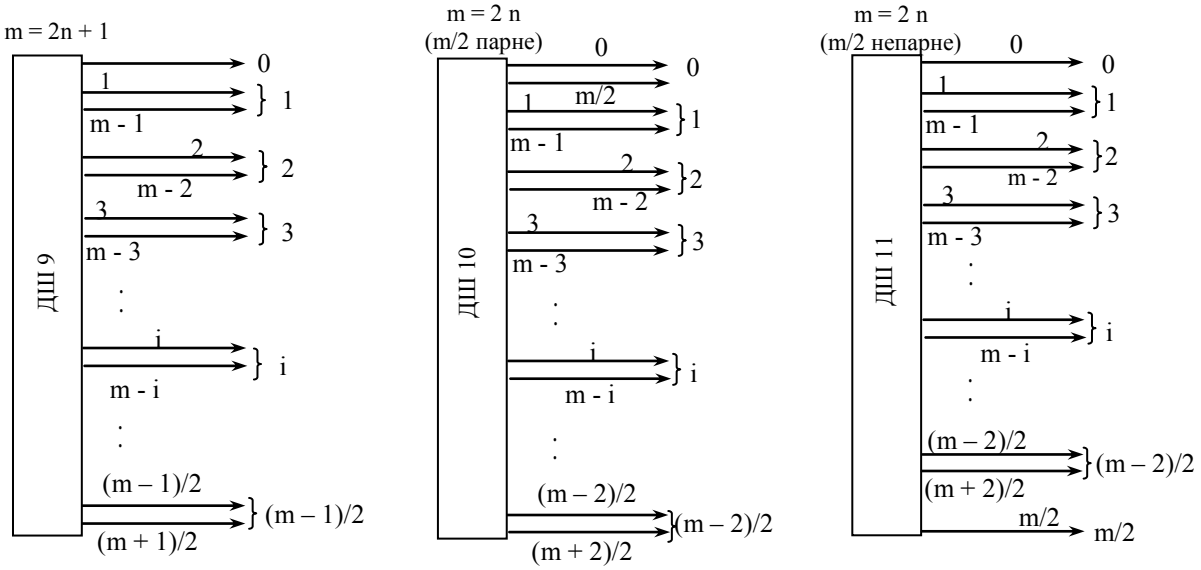

Рис. 2. Алгоритм реалізації операції піднесення чисел до квадрата за довільними модулями m_i МСЧ

Таблиця 1

Реалізація операції $A^2(\mathrm{mod}11)$ (m_1)

Номер пари вихідних шин дешифратора 9	Значення, що призначають парі вихідних шин дешифратора 9	Значення, що призначаються вхідним шинам шифратора 13	Значення, що призначаються вихідним шинам шифратора 13
0	0	0	0000
1	1, 10	1	0001
2	2, 9	4	0100
3	3, 8	9	1001
4	4, 7	5	0101
5	5, 6	3	0011

Таблиця 2

Реалізація операції $A^2 (\mathrm{mod}12)$ (варіант 1, m_2)

Номер пари вихідних шин дешифратора 10	Значення, що призначають парі вихідних шин дешифратора 10	Значення $A^2(\mathrm{mod}12)$, що призначаються вхідним шинам шифратора15	Значення, що призначаються вихідним шинам шифратора 15
0	0,6	0	0000
1	1,11	1	0001
2	2,10	4	0100
3	3,9	9	1001
4	4,8	4	0100
5	5,7	1	0001

Таблиця 3

Реалізація операції $A^2 (\mathrm{mod}14)$ (варіант 2, m_3)

Номер пари вихідних шин дешифратора 11	Значення, що призначають парі вихідних шин дешифратора 11	Значення $A^2(mod14)$, що призначаються вхідним шинам шифратора 17	Значення, що призначаються вихідним шинам шифратора 17
0	0,6	0	0000
1	1,13	1	0001
2	2,12	4	0100
3	3,11	9	1001
4	4,10	2	0010
5	5,9	11	1011
6	6,8	8	1000
7	7	7	0111

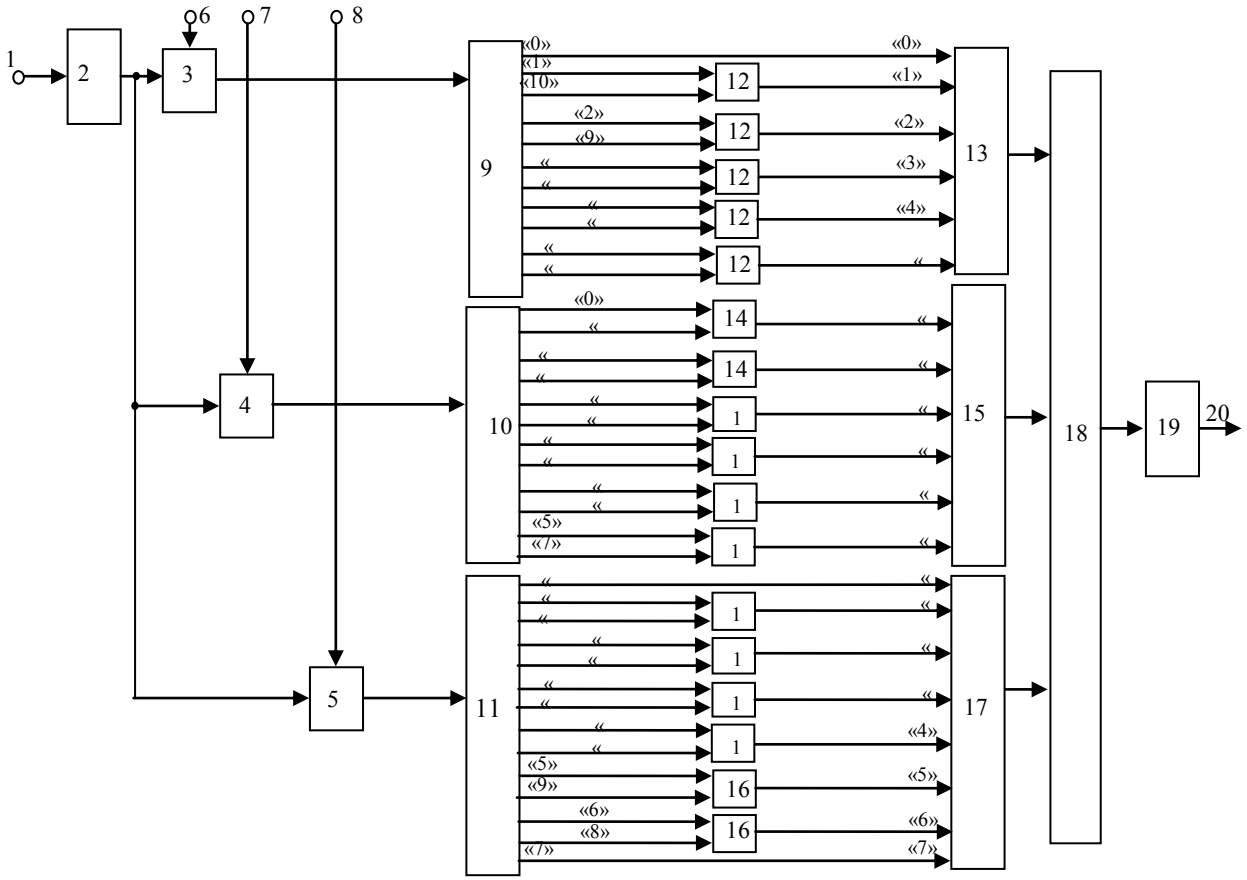

Рис. 3. Пристрій для реалізації операції піднесення чисел до квадрату за заданими модулями m_i МСЧ ($m_1 = 11$, $m_2 = 12$, $m_3 = 14$)

Другий режим. При $m_2 = 12$ - парне число (варіант 1), A = 8 (1000), (рис. 3, 4 і табл. 2). Присутній сигнал шини 7.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи I другої 4 групи число A = 1000 у двійковому коді поступає на восьмий

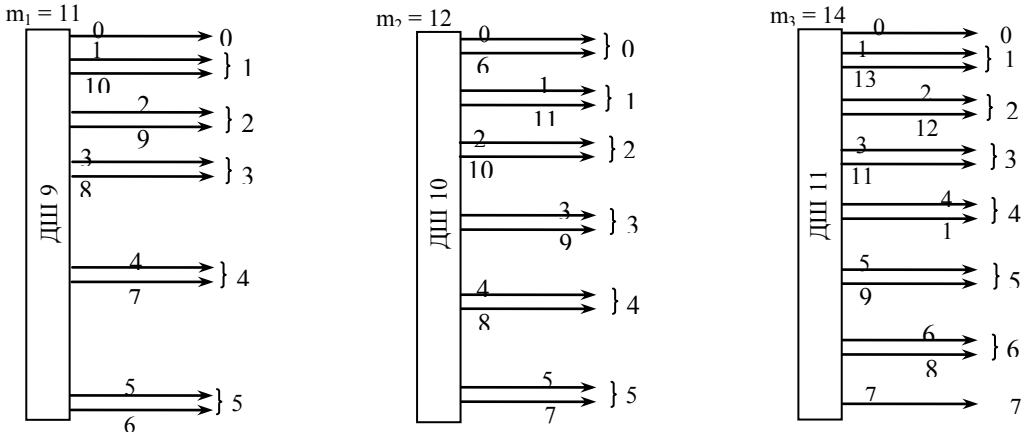

Рис. 4. Алгоритм реалізації операції піднесення чисел до квадрата за заданими модулями m_i МСЧ ($m_1 = 11$, $m_2 = 12$, $m_3 = 14$)

вхід другого дешифратора 10. Дешифратор 10 перетворює число А в унітарний код А = 8, сигнал якого через четвертий елемент АБО другої 14 групи поступає на четвертий вхід другого 15 шифратора. З виходу шифратора 15 результат операції $A^2(\mathrm{mod}\, m_2) = 0100$ в двійковому коді через четверту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою.

Перевірка: $A^2(\mathrm{mod}\, m_2) = 8^2(\mathrm{mod}\, 12) = 4$.

Третій режим. При $m_3 = 14$ парне число (варіант 2), А = 8 (1000), (рис. 3, 4) і табл. 3). Присутній сигнал шини 8.

Пристрій працює наступним чином. За входом 1 через регістр 2, відкриті елементи І третьої 5 групи число А = 1000 у двійковому коді поступає на вхід третього дешифратора 11. Дешифратор 11 перетворює число А в унітарний код А = 8, сигнал якого через шостий елемент АБО третьої 16 групи поступає на восьмий вхід третього 17 шифратора. З виходу шифратора 17 результат операції $A^2(\mathrm{mod}\, m_3) = 1000$ у двійковому коді через четверту 18 групу елементів АБО, регістр 19 поступає на вихід 20 пристрою.

Перевірка: $A^2(\mathrm{mod}\, m_3) = 8^2(\mathrm{mod}\, 14) = 8$.

Висновки

Таким чином, запропонований у даній статті пристрій дозволяє проводити операції $A^2(\mathrm{mod}\, m_i)$ піднесення чисел до квадрата за всіма можливими варіантами модулів m_i МСЧ. Це у свою чергу дає можливість як зниження обчислювальної складності реалізації криптографічного RSA алгоритму, так і підвищити коефіцієнт використання обладнання пристрою для піднесення чисел до квадрата за модулями m_i МСЧ.

Список літератури

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И.. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

2. Барсов В.И. Методология параллельной обработки информации в модулярной системе счисления: моногр. / В.И. Барсов, Л.С. Сорока, В.А. Краснобаев – Х.: МОН, УИПА, 2009.- 288 с.

3. Барсов В.И., Краснобаєв В.А., Сорока Л.С., Загумена К.В., Дугін М.В. Пристрій для піднесення чисел до квадрата за модулями m_i. класу лишків. Пат. 66645 Україна, МПК G06F 7/14. (2006.01) – № и 2011 07927.- 10.01.2012, Бюл. № 1.

4. Барсов В.И. Концепция создания системы быстрой и достоверной обработки криптографической информации на основе использования информационной технологии распределённых вычислений / В.И. Барсов, В.А. Краснобаев, Л.С. Сорока // Збірник наукових праць ХУПС. – Х.: ХУПС, 2012. – Вип. 1 (30).– С. 87 - 92.

Надійшла до редколегії 21.05.2012

Рецензент: д-р техн. наук, проф. І.О. Фурман, Харківський національний технічний університет сільського господарства ім. Петра Василенка, Харків

РЕАЛИЗАЦИЯ МЕТОДА ВЫПОЛНЕНИЯ ОПЕРАЦИИ ВОЗВЕДЕНИЯ ЧИСЕЛ В КВАДРАТ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ МСС

В.И. Барсов

В статье рассмотрена техническая реализация системы криптографической обработки информации на основе использования модулярной системы счисления (МСС), что позволяет уменьшить вычислительную сложность реализации процесса криптографических преобразований, а также повысить эффективность контроля и коррекции ошибок информации.

Ключевые слова: *система обработки криптографической информации, криптографические преобразования, модулярная система счисления.*

REALIZATION OF METHOD OF NUMBERS IN SQUARE ERECTION OPERATION IMPLEMENTATION ON ARBITRARY MNS MODULE

V.I. Barsov

In the article technical realization of the system of cryptographic treatment of information is considered on the basis of the use of the modular number system (MNS) , that allows to decrease calculable complication of realization of process of cryptographic transformations, and also to promote efficiency of control and correction of errors of information.

Keywords: *system of treatment of cryptographic information, cryptographic transformations, modular number system.*