УДК 519.714

В. М. Рудницький, *д.т.н., професор,*
С. В. Бурмістров, *аспірант,*
О. С. Шемшур, *викладач,*
А. М. Тихоненко, *викладач*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна,
sergijburmistrov@yandex.ua

ГРУПИ РЕЛЯТИВНОСТІ БУЛЕВИХ ФУНКЦІЙ В ШИФРУВАЛЬНИХ ПРИСТРОЯХ

В роботі обґрунтовано доцільність побудови модуля шифрування в пристроях, призначених для посимвольного кодування текстової інформації на основі використання властивостей груп релятивності булевих функцій. Це дає можливість зменшити розрядність шини формування поточного фіксованого ключа і суттєво мінімізувати схему по коефіцієнтах S_L *та* S_{AD}.

Ключові слова: *шифрувальні пристрої, функції кодування, функції декодування, фіксований ключ кодування, фіксований ключ декодування, групи релятивності.*

Постановка проблеми. Проблема апаратного шифрування комерційних мереж є однією з ключових при створенні захищених ліній зв'язку. Одним із найперспективніших напрямів вирішення цієї проблеми є модернізація шифрувальних пристроїв (ШП), що працюють за принципом посимвольного кодування машинних кодів. Принцип кодування полягає в заміні одного символу на інший із того ж алфавіту.

Аналіз останніх досліджень і публікацій. Перші промислові зразки ШП з'явилися відразу після закінчення Першої світової війни [1]. В Другу світову війну ці пристрої визначали основу ШП всіх країн, що воювали [2,3,4,5].

Незважаючи на простоту ідеї і досить тривалий термін експлуатації зазначених ШП, побудованих на основі ідеї посимвольного шифрування, цей метод кодування для текстової інформації в модифікованому вигляді має достатньо високий рівень захисту і з успіхом застосовується в комерційних мережах.

Для спрощення викладення суті методу шифрування в модифікованому вигляді візьмемо текстову інформацію, що складається з алфавіту, який містить 8 символів $\{0,1,2,3,4,5,6,7\}$. Нехай ШП передає символи у вигляді бінарних машинних кодів. Для вираження кожного символу всього алфавіту достатньо зобразити символи у вигляді 3-розрядних бінарних машинних кодів (n=3):

$$n = \log_2 8 = 3,$$

де n – кількість аргументів (можуть набувати два види значень – 0 або 1), з яких складається бінарний машинний код

Нехай у результаті використання деякого фіксованого ключа за допомогою шифрувального пристрою відбулося кодування повного алфавіту початкової інформації (табл. 1), де $\{a_0^{\arg}, a_1^{\arg}, ..., a_7^{\arg}\}$ – початкові незакодовані символи, а $\{a_0^{in}, a_1^{in}, ..., a_7^{in}\}$ – відповідні їм закодовані символи.

Стовпчики бінарних кодів початкового символу визначають номери початкових функцій аргументів $\{f_3^{\arg}, f_2^{\arg}, f_1^{\arg}\}$, де номерами функцій у цьому випадку є:

$$f_3^{\arg} = 11110000_{BIN} = 240_{DEC} = F0_{HEX},$$
$$f_2^{\arg} = 11001100_{BIN} = 204_{DEC} = CC_{HEX},$$
$$f_1^{\arg} = 10101010_{BIN} = 170_{DEC} = AA_{HEX}.$$

Аналогічно, стовпчики бінарних векторів передаваного символу є номерами функцій кодування $\{f_1^{in}, f_2^{in}, f_3^{in}\}$. Саме повний набір зазначених функцій кодування і визначає номер фіксованого ключа, за допомогою якого здійснюється шифрування інформації. Для обробки бінарних машинних кодів, що містять n символів, оптимальним значенням кількості функцій кодування в номері фіксованого ключа є значення n.

Таблиця 1

Один із варіантів кодування інформації за допомогою фіксованого ключа

№ початкового символу	Бінарний код початкового символу			Бінарний код передаваного символу			№ передаваного символу
$a_0^{\arg}$	0	0	0	0	1	1	$a_0^{in} = a_3^{\arg}$
$a_1^{\arg}$	0	0	1	1	1	0	$a_1^{in} = a_6^{\arg}$
$a_2^{\arg}$	0	1	0	0	0	1	$a_2^{in} = a_1^{\arg}$
$a_3^{\arg}$	0	1	1	1	1	1	$a_3^{in} = a_7^{\arg}$
$a_4^{\arg}$	1	0	0	0	1	0	$a_4^{in} = a_2^{\arg}$
$a_5^{\arg}$	1	0	1	0	0	0	$a_5^{in} = a_0^{\arg}$
$a_6^{\arg}$	1	1	0	1	0	0	$a_6^{in} = a_4^{\arg}$
$a_7^{\arg}$	1	1	1	1	0	1	$a_7^{in} = a_5^{\arg}$
	$\uparrow$ $f_3^{\arg}$	$\uparrow$ $f_2^{\arg}$	$\uparrow$ $f_1^{\arg}$	$\uparrow$ f_1^{in}	$\uparrow$ f_2^{in}	$\uparrow$ f_3^{in}	
	Початкові функції аргументів			Функції кодування			

Метод шифрування з фіксованим ключем у модифікованому вигляді полягає у використанні для кожного наступного символу текстової інформації нового набору функцій кодування $\{f_1^{in}, f_2^{in}, f_3^{in}\}$.

Початкові функції аргументів $\{f_3^{\arg}, f_2^{\arg}, f_1^{\arg}\}$ мають в своїх бінарних кодах однакову кількість нулів та одиниць. В процесі кодування інформації виконується заміна символ на символ, тобто переставляються в таблиці тільки рядки, і, як наслідок, кількість одиниць у стовпчиках, інакше кажучи, в функціях кодування $\{f_1^{in}, f_2^{in}, f_3^{in}\}$ не змінюється. Тому деякою функцією кодування f_{i}^{in} із набору $\{f_1^{in}, f_2^{in}, f_3^{in}\}$ є не довільна булева функція, що містить 2^n символів у бінарному векторі, а лише та, що має однакову кількість нулів і одиниць. Для n=3 таких функцій кодування бінарних векторів – 70, а кількість номерів фіксованого ключа наборів функцій кодування становить $2^n!$ – більше 40 000 комбінацій.

Користуючись описаними вище міркуваннями, пристрій кодування повинен містити такі блоки (рис. 1):

- блок формування поточного фіксованого ключа, основне призначення якого – задати на кожен із трьох модулів шифрування *M1*, *M2* і *M3* відповідну функцію кодування f_{i}^{in} із набору $\{f_1^{in}, f_2^{in}, f_3^{in}\}$ поточного фіксованого ключа;
- модулі шифрування *M1*, *M2* і *M3* відповідної функції кодування, що побітово шифрують символи. За структурною будовою всі три модулі є ідентичними

Із усіх блоків пристрою секретним є лише блок формування поточного фіксованого ключа. Тому при розробці схеми пристрою дотримано один із основних принципів побудови шифрувальних пристроїв – розкриття загальної будови пристрою та будови решти блоків не дає можливості вільно читати закодовані сповіщення.

Формулювання цілей статті. Основною технічною проблемою під час розробки кодувальних пристроїв, що реалізують метод шифрування з фіксованим ключем у модифікованому вигляді, є розробка схеми модуля шифрування. Цей модуль має містити повний перелік функцій кодування f_{i}^{in} для вказаного числа n, що містять однакову кількість нулів і одиниць. Лавиноподібне зростання кількості булевих функцій (БФ) навіть при незначному зростанні числа n робить реалізацію цього модуля досить проблематичною (табл. 2). Тому виникає необхідність пошуку технічних рішень для суттєвого об'єднання схем реалізації функцій кодування f_{i}^{in} в інтегровані схеми.

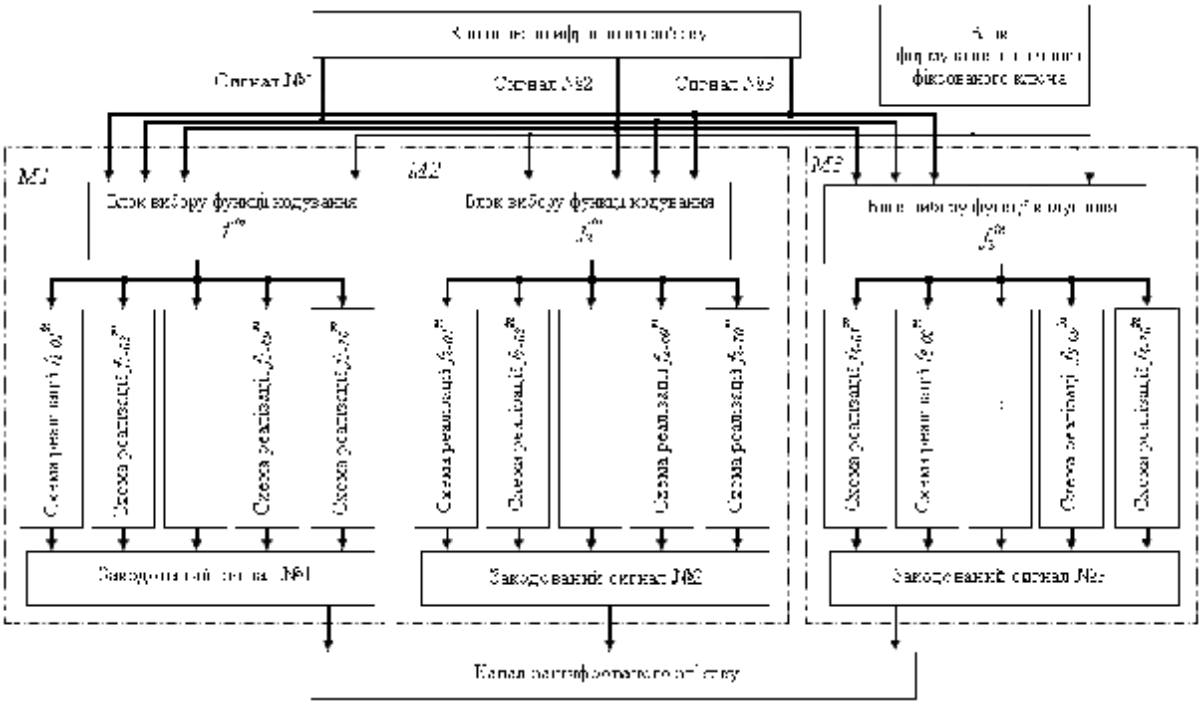

Рис. 1. Загальна схема пристрою кодування 3-розрядних машинних кодів

Тому **актуальним питанням** під час розробки пристрою в цілому є оптимізація будови модуля шифрування, пов'язана з побудовою структурної схеми модуля, який би містив суттєво меншу кількість структурних елементів усередині модуля. Потрібно на рівні БФ знайти такі структурні множини, які б за спільними ознаками суттєво об'єднали БФ у більш глобальні структури.

Таблиця 2

Залежність зростання кількості наборів функцій кодування f_i^{in} при зростанні числа *n*

№ п/п	Кількість змінних *n* у функції кодування f_i^{in}	Кількість наборів функцій кодування $\{f_1^{in}, f_2^{in}, ..., f_n^{in}\}$
1	2	24
2	3	40320
3	4	$2{,}09228*10^{13}$
4	5	$2{,}63131*10^{35}$
5	6	$1{,}26887*10^{89}$

Основною метою роботи є розробка схеми модуля шифрування ШП на основі застосування властивостей більш глобальних множин у повній множині БФ *L(n)*, що об'єднують БФ за їх спільними властивостями. При цьому повинна бути забезпечена максимальна швидкодія пристрою.

Виклад основного матеріалу. Проблема об'єднання БФ у більш глобальні структури описана в [6, 7].

Властивість об'єднання БФ дає можливість ефективно об'єднати функції кодування в межах одного модуля в більш глобальну структуру (табл. 3), що має назву групи релятивності (ГР) [8].

Групи релятивності – це підмножини в повній множині БФ *L(n)*, що складаються із БФ, які отримуються одна з іншої шляхом перенумерації та інвертуванням аргументів x_i БФ.

Таблиця 3

Співвідношення наповнення повної множини *L(n)* булевими функціями та групами релятивності

К-сть x_i БФ в *L(n)*	Кількість БФ в *L(n)*	Кількість ГР в *L(n)*
2	2^4=16	5
3	2^8=256	22
4	2^{16}=65.536	402
5	2^{32}=4.294.967.296	1.228.158
6	$2^{64} \approx 1{,}84467 \cdot 10^{19}$	400.507.806.843.728

Номер ГР дорівнює найменшому номеру БФ, що належить даній групі.

Важливою конструктивною деталлю є те, що всі елементи ГР в оптимізованій формі мають однакові показники складності реалізації і відрізняються один від одного лише поляризаційними входами.

З практичної точки зору, ця властивість ГР дає можливість інтегрувати всі БФ, що належать одній ГР [9, 10], в одну електричну схему, в якій за допомогою зовнішнього керування шляхом переключення сигналів на вхідній шині можна вибирати потрібну БФ.

Основною властивістю, що об'єднує всі БФ, які належать наборам функцій кодування $\{f_1^{in}, f_2^{in}, ..., f_n^{in}\}$, є будова їх бінарних векторів, а саме той факт, що всі БФ мають у векторі однакову кількість нулів і одиниць. Повна множина $L(3)$ булевих функцій, що включають три аргументи, містить 70 БФ, в яких у бінарному векторі є однакова кількість нулів і одиниць. Ці БФ об'єднуються в шість ГР (табл. 4).

Таблиця 4

Склад груп релятивності в множині $L(3)$ булевих функцій, в яких у бінарному векторі є однакова кількість нулів і одиниць

№ п/п	№ ГР	К-сть БФ, які входять в ГР	№ БФ, що належать ГР
1	15	6	15, 51, 85, 170, 204, 240
2	23	8	23, 43, 77, 113, 142, 178, 212, 232
3	27	24	27, 29, 39, 46, 53, 58, 71, 78, 83, 92, 114, 116, 139, 141, 163, 172, 177, 184, 197, 202, 209, 216, 226, 228
4	30	24	30, 45, 54, 57, 75, 86, 89, 99, 101, 106, 108, 120, 135, 147, 149, 154, 156, 166, 169, 180, 198, 201, 210, 225
5	60	6	60, 90, 102, 153, 165, 195
6	105	2	105, 150

Як наслідок, модулі шифрування *M1*, *M2* і *M3*, що побітово шифрують символи, повинні містити не 70 блоків схем реалізацій БФ f_{i}^{in}, а лише шість схем реалізацій ГР БФ f_{i}^{in}. Відповідно, блок вибору функції кодування повинен вибирати як потрібну ГР, так і відповідну БФ усередині ГР.

Кожна схема реалізацій ГР БФ f_{i}^{in} має власне умовне ядро та систему включення відповідної схеми, що реалізує конкретну БФ із складу ГР.

Так, для прикладу, ГР № 23 містить вісім БФ (див. табл. 4). Ядром, що реалізує цю ГР, є дворівнева схема базисів І, АБО, НЕ, що містить шість входів $c_{i.j}$, кожен з яких, залежно від номера потрібної БФ, приєднується до прямого або інверсного сигналу конкретного аргументу вхідної шини (рис. 2).

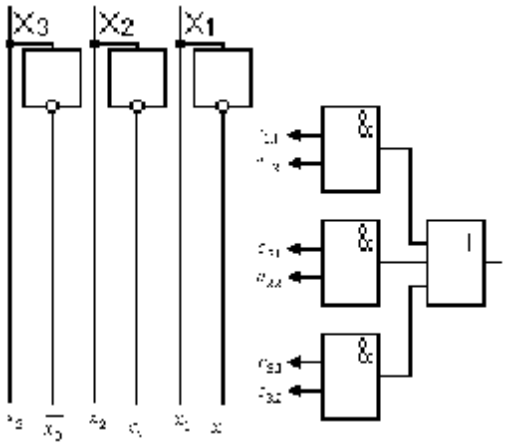

Рис. 2. Об'єднана схема для спільної реалізації всіх булевих функцій ГР № 23

Схема підключення входів $c_{i.j}$ для реалізації довільної БФ зі складу ГР наведена в табл. 5.

Таблиця 5

Контакти підключення поляризаційних входів в об'єднаній схемі

№ п/п	№ БФ	Підключення поляризаційних входів					
		$c_{1.1}$	$c_{1.2}$	$c_{2.1}$	$c_{2.2}$	$c_{3.1}$	$c_{3.2}$
1	23	$\overline{x_3}$	$\overline{x_2}$	$\overline{x_3}$	$\overline{x_1}$	$\overline{x_2}$	$\overline{x_1}$
2	43	$\overline{x_3}$	$\overline{x_2}$	$\overline{x_3}$	x_1	$\overline{x_2}$	x_1
3	77	$\overline{x_3}$	x_2	$\overline{x_3}$	$\overline{x_1}$	x_2	$\overline{x_1}$
4	113	x_3	$\overline{x_2}$	x_3	$\overline{x_1}$	$\overline{x_2}$	$\overline{x_1}$
5	142	$\overline{x_3}$	x_2	$\overline{x_3}$	x_1	x_2	x_1
6	178	x_3	$\overline{x_2}$	x_3	x_1	$\overline{x_2}$	x_1
7	212	x_3	x_2	x_3	$\overline{x_1}$	x_2	$\overline{x_1}$
8	232	x_3	x_2	x_3	x_1	x_2	x_1

Слід зазначити, що роль блоку вибору функції кодування f_i^{in} суттєво відрізняється в оптимізованій схемі. Блок вибору функцій кодування f_i^{in} призначений для підключення поляризаційних входів до ядра ГР. Цей блок повинен вибирати як потрібну ГР, так і потрібну БФ усередині ГР.

Для 3-розрядних кодів для вибору потрібної ГР потрібно мати:

$$2^{l_1} \geq N_{GR},$$

$$l_1 \geq \log_2 N_{GR} = \log_2 6 \geq 3,$$

де l_1 – кількість управляючих електродів для вибору потрібної ГР, N_{GR} – кількість ГР.

Для вибору потрібної БФ усередині ГР потрібно мати:

$$l_2 \geq \log_2 N_{BF} = \log_2 24 \geq 5,$$

де l_2 – кількість управляючих електродів для вибору потрібної ГР, N_{BF} – максимальна кількість БФ усередині ГР.

Тому шина, що з'єднує блок формування поточного фіксованого ключа з модулями шифрування *M1*, *M2* і *M3*, повинна бути 24-розрядною (три модулі по три розряди для вибору відповідної ГР та по п'ять розрядів для вибору відповідної БФ). Саме, виходячи з цих міркувань, і будується таблиця кодів, що управляють процесом кодування символів. Ця таблиця служить основою для побудови мультиплексорів, що суміщають вхідні шини, по яких подається вхідний сигнал, з власним умовним ядром ГР.

В результаті загальна оптимізована схема пристрою кодування 3-розрядних машинних кодів має вигляд (рис. 3). Вказана компоновка модуля шифрування дає можливість суттєво мінімізувати схему.

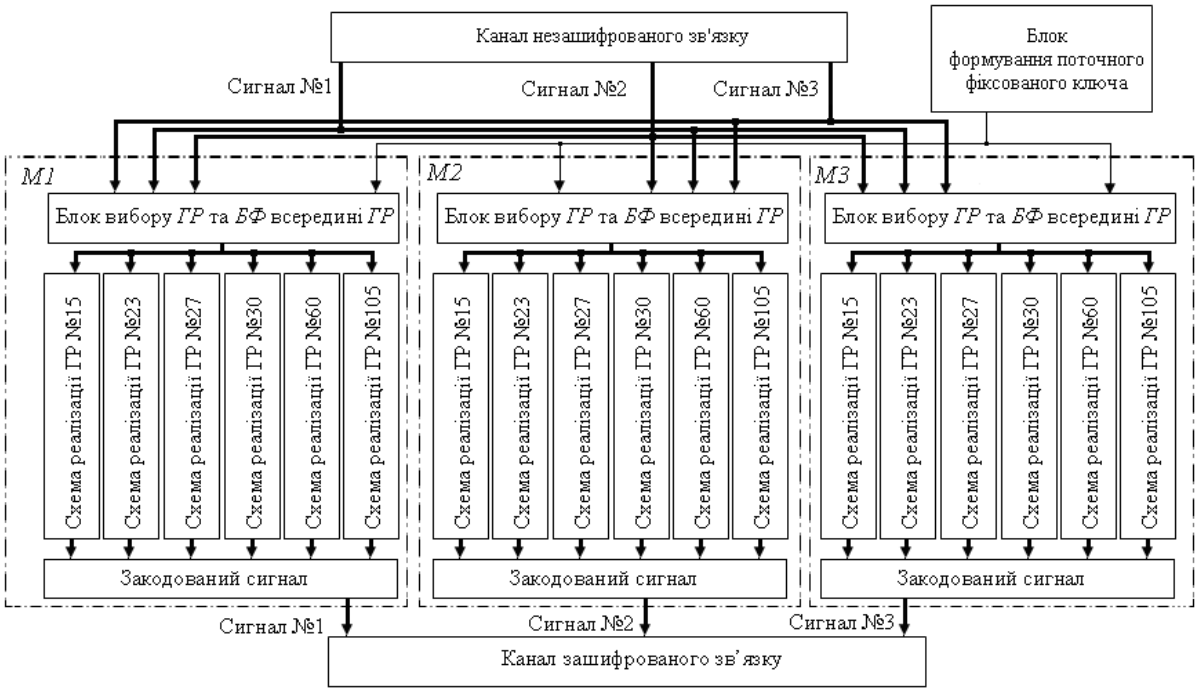

Рис. 3. Загальна оптимізована схема пристрою кодування 3-розрядних машинних кодів

Схема має досить високий рівень швидкодії. Сигнал під час шифрування проходить послідовно спочатку каскад поляризації, потім два каскади мультиплексорів та два каскади умовного ядра ГР БФ – всього п'ять каскадів. Тому час затримки сигналу повинен бути мінімальний.

Порівняно з класичною програмованою логічною матрицею досягається мінімізація схеми по коефіцієнтах: кількість літерал S_L становить 9,69 разу, кількість доданків S_{AD} – 2,27 разу.

Висновки:

1. В роботі обґрунтовано схему модуля шифрування ШП на основі застосування властивостей ГР БФ, що об'єднують БФ за їх спільними властивостями.
2. Нова схема дає можливість зменшити розрядність шини формування поточного фіксованого ключа та суттєво мінімізувати схему по коефіцієнтах S_L – 9,69 разу, та S_{AD} – 2,27 разу.

Список літератури

1. Адаменко М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. – М. : ДМК-Пресс, 2012. – 256 с.
2. Черняк Л. Тайны проекта Ultra / Леонид Черняк // Открытые системы. – 2003. – № 07. − С. 87–92.
3. Черняк Л. Тайны проекта Ultra / Леонид Черняк // Открытые системы. – 2003. – № 08. − С. 89–95.
4. Смарт Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова, под ред. С. К. Ландо. – М. : Техносфера, 2005. – 528 с. – (Серия : Мир программирования).
5. Colossus: The First electronic computer: the secrets of Bletchley Park's code-breaking computers / B. Jack Copeland OUP Oxford, 2006. – 462 p.
6. Бибило П. Н Синтез комбинационных схем методами функциональной декомпозиции / П. Н. Бибило, С. В. Енин ; под ред. А. Д. Закревского. – Мн. : Наука и техника, 1987. – 189 с., ил.
7. Артюхов В. Л. Настраиваемые модули для управляющих логических устройств. / Артюхов В. Л., Копейкин Г. А., Шалыто А. А. – Л. : Энергоиздат, 1981. – 165 с.
8. Кочкарьов Ю. О. Моделі і методи вирішення «проблеми каталогізації логічних функцій» / Ю. О. Кочкарьов, С. В. Бурмістров, І. В. Синько // Вісник Черкаського державного технологічного університету. – 2012. – № 1. − С. 32–34.
9. Кочкарьов Ю. О. Проблеми інформаційного ущільнення множин логічних функцій (ЛФ) / Ю. О. Кочкарьов, С. В. Бурмістров, І. В. Синько // Вісник Черкаського університету. – 2012. – № 18 (231) − С. 93–97. – (Серія : Прикладна математика. Інформатика).
10. Кочкарьов Ю. О. Спрощення логічного синтезу цифрових блоків на основі каталогів логічних функцій / Ю. О. Кочкарьов, С. В. Бурмістров, І. В. Синько // Радиоэлектроника и информатика. – 2012. – № 2 (57). − С. 67–69.

References

1. Adamenko, M. V. (2012) Fundamentals of classical cryptology: secrets of encrypts and codes. Moscow: DMK-Press, 256 p. [in Russian].
2. Chernyak, L. (2003) Secrets of Ultra project. *Otkrytye sistemy*, (07), pp. 87–92 [in Russian].
3. Chernyak, L. (2003) Secrets of Ultra project. *Otkrytye sistemy*, (08), pp. 89–95 [in Russian].
4. Smart, N. (2005) Cryptography. Transl. from Engl. S. A. Kuleshov. In: S. K. Lando (Ed.). Moscow: Technosfera, 528 p. The series "World of programming" [in Russian].
5. Colossus: The first electronic computer: the secrets of Bletchley Park's code-breaking computers (2006). B. Jack Copeland OUP Oxford, 462 p.
6. Bibilo, P. N. and Enin, S. V. (1987) Synthesis of combinational circuits by functional decomposition methods. In: A. D. Zakrevskiy (Ed.). Minsk: Nauka i tehnika, 189 pp., ill. [in Russian].
7. Artyuhov, V. L. Kopeykin, G. A. and Shalyto, A. A. (1981) Custom modules for control logic devices. Leningrad: Energoizdat, 165 p. [in Russian].
8. Kochkarev ,Yu. O., Burmistrov, S. V. and Syn'ko, I. V. (2012) Models and methods for solving of "the problem of logic functions cataloging". *Visnyk Cherkas'kogo derzhavnogo tehnologichnogo universytetu,* (1), pp. 32–34 [in Ukrainian].

9. Kochkarev, Yu. O., Burmistrov, S. V. and Syn'ko, I. V. (2012) Problems of information sealing of logic functions (LF) sets. *Visnyk Cherkas'kogo universytetu. Seriya: Prykladna matematika. Informatyka*, 18 (231). pp. 93–97 [in Ukrainian].
10. Kochkarev, Yu. O., Burmistrov, S. V. and Syn'ko, I. V. (2012) Simplifying of logic synthesis of digital blocks based on logic functions catalogues. Radioelektronika i informatika, 2 (57), pp. 67–69 [in Ukrainian].

V. M. Rudnyts'kyy, *D.Sc., professor,*
S. V. Burmistrov, *postgraduate student,*
O. S. Shemshur, *lecturer,*
A. M. Tykhonenko, *lecturer*
Cherkassy state technological university,
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine
sergijburmistrov@yandex.ua

GROUPS OF BOOLEAN FUNCTIONS RELATIVITY IN ENCRYPTION DEVICES

The problem of hardware encryption of commercial networks is one of key problems in creating of secure communication lines. The modernization of encryption devices, which operate on the principle of character-oriented encoding of machine codes is one of the most promising directions for solving of this problem. The principle of coding consists in the replacement of one character to another with the same letters.

In the article the structure of one of the key modules of encryption device for encoding of text information is considered.

The designed module is based on encryption through the use of properties of Boolean functions subsets – groups of relativity. This allows to merge into one unified scheme for large groups of Boolean functions belonging to the same group of relativity in both coding functions.

Statistical studies have shown that as encoding functions can act only Boolean functions, which in its own binary codes have the same number of digits "0" and "1". This fixed encryption key is formed from all possible combinatorial variants od encoding feature sets, provided that there are no two identical sets of functions.

The peculiarity of the combined scheme is that it contains a single nucleus. The choice of desired function encoding is performed using multiplex switching inputs of core polarization.

New scheme makes it possible to reduce the size of the bar for formation of current fixed key and to significantly minimize the scheme according to S_L *and* S_{AD} *coefficients.*

Keywords: *encryption devices, encoding functions, decoding functions, fixed encryption key, fixed decoding key, groups of relativity.*

Рецензенти: С. М. Первунінський, д.т.н., професор, .
С. В. Голуб, д.т.н., професор.