**УДК 681.3.06**

**О. М. БЕВЗ[1], А. О. ЯРОВЕНКО[1]**

# ПІДВИЩЕННЯ СТІЙКОСТІ ШИФРУВАННЯ ІНФОРМАЦІЇ В ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМАХ БЛОЧНИМИ ШИФРАМИ НА ОСНОВІ ВИКОРИСТАННЯ БАГАТОРІВНЕВИХ ГНІЗДОВИХ ПІДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ

[1]***Вінницький національний технічний університет,***
***21021, Хмельницьке шосе, 95, м. Вінниця, Україна,***
***E-mail: ezorf@mail.ru***

**Анотація.** У даній статті запропоновано шифрувальне перетворення, що складається із лінійного та нелінійного шарів. Лінійний шар реалізовано гніздової підстановочно-перестановочною мережею. Мережа складається із трьох рівнів — нижнього, середнього і верхнього. Кожен із рівнів реалізовано кодом із максимальною відстанню. Доведено збільшення кількості активних блоків підстановки (S-боксів) для перетворень, що використовують даний тип лінійного шару. Розглянуто варіанти реалізації шифрувальних перетворень із підстановочно-перестановочними мережами даного типу, довжиною 8 і 16 біт, і визначено варіанти реалізації з найбільшою стійкістю шифрування.

**Аннотация.** В данной статье предложено шифровальное преобразование, состоящее из линейного и нелинейного слоев. Линейный слой реализован гнездовой подстановочно-перестановочной сетью. Сеть состоит из трех уровней — нижнего, среднего и верхнего. Каждый из уровней реализован кодом с максимальным расстоянием. Доказано увеличение количества активних блоков подстановки (S-боксов) для преобразований, использующих данный тип линейного слоя. Рассмотрены варианты реализации шифровальных преобразований с подстановно-перестановочными сетями данного типа для S-боксов, длинною 8 и 16 бит, и определены варианты реализации с найбольшей стойкостью шифрования.

**Abstract.** This article contains cipher transformation that consists of linear and nonlinear layers. The linear layer is constructed with the usage of nested substitution-permutation network. The network consists of three levels: the low level, the middle level and the high level. Each of the levels uses maximal distance codes. The increasing of number of active S-boxes for this transformation that are using this king of linear layer is proved. The variants of realization of the cipher transformation which uses substitution-permutation network for 8×8 and 16×16-bit S-boxes are considered. The variant of realization with the highest cryptography security is defined.

**Ключові слова:** Підстановочно-перестановочна мережа, коди з максимальною відстанню, стійкість шифрування, активні S-бокси, довжина слова кода.

## ВСТУП

У зв’язку із постійним збільшенням обсягу передавання інформації оптико-електронними системами збільшуються спроби несанкціонованого доступу до них. Тому вирішення проблеми підвищення ефективності шифрування в оптико-електронних системах є актуальною задачею. Велика кількість сучасних алгоритмів блочного шифрування використовує архітектуру підстановочно-перестановочних мереж (Substitution-Permutation Networks — SPN). Головний криптографічний параметр протидії зламу блочного шифру — значення стійкості. Стійкість блочного шифру визначає кількість інформації, яка необхідна для визначення ключа шифрування. Стійкість блочних шифрів і, зокрема, блочних шифрів на основі підстановочно-перестановочних мереж залежить від кількості раундів шифрування та від стійкості компонентів, які утворюють раунд. Гніздові підстановочно-перестановочні мережі — тип SPN-мереж, які демонструють високі показники криптографічної стійкості. Зважаючи на те, що швидкість передавання та обробки інформації постійно підвищується, і по цій причині потужність програмних засобів, які використовуються для зламу блочних шифрів, необхідно розробляти в оптоелектронних системах нові блочні шифри з більш високою криптографічною стійкістю.

*Метою цієї статті* є підвищення стійкості шифрування блочного шифру на основі криптографічного перетворення, що реалізується SPN –мережею з S-боксами розміром 16 на 16 біт в оптоелектронних системах.

## ПОСТАНОВКА ЗАВДАННЯ

Для підвищення числового значення стійкості шифрування в оптико-електронних системах підстановочно-перестановочними мережами слід обрати показник, який буде визначати коефіцієнт протидії блочного шифру до певного типу криптоаналізу. Найпотужнішими типами криптоаналізу є лінійний та диференційний. Одним із головних факторів, які впливають на стійкість блочного шифру до цих типів криптоаналізу, є кількість активних S-боксів. По цій причині необхідно розробити блочний шифр, який буде мати більшу кількість активних S-боксів в одому раунді шифрування, ніж існуючі аналоги.

## ВІДОМІ ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ

Існують наступні шляхи збільшення кількості активних S-боксів:

— в роботі [1] запропоновано в раунді шифрування використовувати гніздові підстановочно-перестановочні мережі;

— в роботі [2] розширено використання гніздових підстановочно-перестановочних мереж на шифри з довжиною S-боксу 16 біт.

## РОЗВ'ЯЗАННЯ

Розв'язок завдання представимо у трьох кроках. На першому кроці визначимо залежність криптографічної стійкості одного раунду перетворення від значення криптографічної стійкості компонентів, що його утворюють. На другому кроці запропонуємо нову структуру для одного раунду гніздової підстановочно-перестановочної мережі. На третьому кроці визначимо значення криптографічної стійкості і порівняємо з існуючими.

Відповідно до постановки завдання представимо перший крок. Гніздова SPN-мережа — це підстановочно-перестановочна мережа, яка складається з певної кількості раундів. В кожному раунді шифрувального перетворення гніздової мережі застосовуються два рівні — верхній та нижній. Використання двох рівнів в кожному раунді необхідне для збільшення кількості активних S-боксів [3]. Кількість активних S-боксів — це один із факторів, який впливає на протидію лінійному та диференційному криптоаналізу та який визначає стійкість шифру. Для максимальної кількості активних S-боксів на двох рівнях SPN-мережі застосовують коди з максимальною відстанню — КМВ. Так на верхньому рівні застосовують код з максимальною відстанню $КМВ_В$, а на нижньому рівні — $КМВ_Н$. Для SPN-мереж з такою організацією раундів кількість активних S-боксів дорівнює [3]:

$$N = (m_2 + 1)(m_1 + 1), \tag{1}$$

де $m_2$ — довжина слова $КМВ_Н$,

$m_1$— довжина слова $КМВ_В$.

По тій причині, що коди з максимальною відстанню впливають на кількість активних S-боксів та, відповідно, стійкість шифрування, необхідно проаналізувати їхню структуру та визначити її вплив на формування кількості активних S-боксів.

Код КМВ ($2m$, $m$, $m + 1$) — код з твірною матрицею $G = [I] \cdot [C]$, де $C$ — твірна матриця розміром $m \times m$, $I$ — одинична матриця, $m$ — довжина слова кода [4]. В блочних шифрах, які реалізовані на основі гніздових SPN-мереж використовується лише твірна матриця — $C$.

Перетворення, яке реалізовано на одному рівні гніздової SPN-мережі визначає відображення результату перетворення S-боксів $X$ в двійковий вектор $Y$ через добуток матриць над полем Галуа — $GF(2^n)$. Порядок поля Галуа – $n$ визначає довжину S-боксу.

$$\begin{bmatrix} y_0 \\ \vdots \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} & \cdots & c_{0,m-1} \\ \vdots & c_{i,j} & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,m-1} \end{bmatrix} \times \begin{bmatrix} x_0 \\ \vdots \\ x_{m-1} \end{bmatrix}, \tag{2}$$

де $x_j$ — результуюче значення певного S-боксу, $x_j \in GF(2n)$;

$y_j$ — результуюче значення певного рівня гніздової SPN, $y_j \in GF(2^n)$;

$c_{ij}$ — коефіцієнти твірної матриці КМВ-перетворення, $c_{ij} \in GF(2^n)$;

$m$ — довжина слова кода.

З аналізу виразів (1) та (2) очевидно, що кількість активних S-боксів прямим чином залежить від довжини слова КМВ-перетворення верхнього та нижнього рівнів, що, в свою чергу, залежить від розміру S-боксу та довжини блоку шифрування. В роботі [5] визначено значення максимальної кількості активних S-боксів шифрувального перетворення довжиною 64 біта для S-боксів різної довжини. В роботі [6] визначено значення максимальної кількості активних S-боксів в шифрувальному перетворенні довжиною 128 біт для S-боксів різної довжини. Відповідно до постановки завдання необхідно виконати

формування перетворення одного раунду з більшим значенням стійкості до лінійного та диференційного криптоаналізу. З урахуванням вище наведеного та по причині того, що стійкість залежить від кількості активних S-боксів, дослідження необхідно проводити в напрямку формування перетворення, в якому кількість активних S-боксів буде більшою за шифрувальні перетворення одного раунду в існуючих блочних шифрах з гніздовою SPN-мережею.

По тій причині, що кількість активних S-боксів залежить від перетворень, що здійснюються на кожному рівні, і кожний рівень впливає на формування та кількість активних S-боксів, то доцільно розглянути раунд перетворення з більшою кількістю рівнів. Причиною підвищення кількості активних S-боксів буде внесення впливу кожного рівня на загальну кількість активних S-боксів. Розглянемо раунд перетворення, в якому використовується три рівні — верхній, середній та нижній. В цьому випадку на нижньому рівні буде застосований код $КМВ_Н$, на середньому рівні код — $КМВ_С$, і на верхньому рівні — $КМВ_В$. Визначення кількості активних S-боксів такого раунду буде визначатися наступною теоремою.

**Теорема.** Кількість активних S-боксів раундового перетворення, що складається із трьох рівнів (верхнього, середнього і нижнього), на кожному з яких застосовані коди з максимальною відстанню з довжиною слова $m_1$ — на нижньому рівні, $m_2$ — на середньому та $m_3$ — на верхньому, становить:

$$N = (m_3 + 1)(m_1 m_2 + m_1 + m_2 + 2) \quad . (3)$$

Доведення. Розглянемо два нижніх рівня раундового перетворення, як один рівень. Припустимо, що кількість активних S-боксів такого рівня буде становити $M$. Тоді кількість активних S-боксів раунду, відповідно до виразу (1):

$$N = (m_3 + 1)(M + 1) \quad (4)$$

Але сукупна кількість активних S-боксів — $M$ двох нижніх рівнів відповідно до виразу (1) визначиться виразом:

$$M = (m_2 + 1)(m_1 + 1). \quad (5)$$

Після підстановки значення кількості активних S-боксів двох нижніх рівнів $M$ у вираз (4):

$$N = (m_3 + 1)((m_2 + 1)(m_1 + 1) + 1) = (m_3 + 1)(m_1 m_2 + m_1 + m_1 + 2) \quad (6)$$

**Теорему доведено.**

На рисунку 1 наведено раунд підстановочно-перестановочної мережі, в якому застосовуються три рівня перестановок.

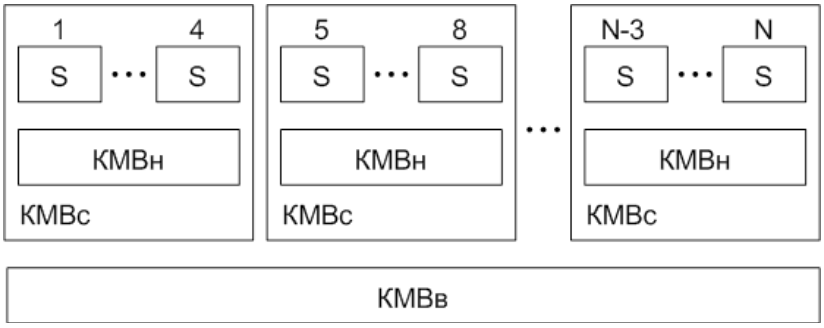


Рис. 1. Один раунд підстановочно-перестановочної мережі з трьома рівнями перестановок

По тій причині, що, в залежності від довжини блоку раундового перетворення та розміру S-боксів можливо використовувати коди з максимальною відстанню з різною довжиною слова і, відповідно, різним значенням кількості активних S-боксів, необхідно розглянути всі можливі варіанти та вибрати той, в якому кількість активних S-боксів буде приймати максимальне значення.

Найбільш поширеним розміром S-боксів у сучасних блочних шифрах є розмір — 8 біт [7, 8]. Так, як стійкість S-боксу пропорційна його довжині [9] і по причині того, що розрядність процесорів, які використовуються в оптоелектронних системах складає 64 та 128 біт, то перспективним напрямом є застосування та формування S-боксів, розміром 16 біт [2]. Тому необхідно розглянути всі можливі варіанти трьохрівневих гніздових SPN-мереж з розміром S-боксу 8 та 16 біт та визначити кількість активних S-боксів одного раунду.

В таблиці 1 наведені всі можливі варіанти трьохрівневих гніздових підстановочно-перестановочних мереж з довжиною блоку — 128 біт, в яких застосовані S-бокси розміром 8 біт, та визначена відповідна кількість активних S-боксів одного раунду.

В таблиці 2 наведені всі можливі варіанти трьохрівневих гніздових підстановочно-перестановочних мереж з довжиною блоку — 128 біт, в яких застосовані S-бокси розміром 16 біт, та визначена відповідна кількість активних S-боксів одного раунду.

З аналізу таблиць 1 та 2 очевидно, що серед SPN мереж, в яких розмір S-боксу становить 8 біт максимальну кількість активних S-боксів формує SPN мережа з $КМВ_В$ = (2,1,2), $КМВ_С$ = (2,1,2) та $КМВ_Н$ = (32,16,17), і ця кількість становить — 85. В SPN мережі з S-боксами розміром 16 біт максимальна кількість активних S-боксів буде реалізована SPN мережею з $КМВ_В$ = (2,1,2), $КМВ_С$ = (2,1,2) та $КМВ_Н$ = (16,8,9), і ця кількість становить — 45.

Таблиця 1.

**Залежність кількості активних S-боксів від типу SPN-мережі довжиною 128 біт з трьома рівнями і розміром S-боксу — 8 біт**

| Номер варіанту | Тип КМВ нижнього рівня | Тип КМВ середнього рівня | Тип КМВ верхнього рівня | Кількість активних S-боксів |
|---|---|---|---|---|
| 1 | (2,1,2) | (2,1,2) | (32,16,17) | 85 |
| 2 | (2,1,2) | (4,2,3) | (16,8,9) | 63 |
| 3 | (2,1,2) | (8,4,5) | (8,4,5) | 55 |
| 4 | (2,1,2) | (32,16,17) | (2,1,2) | 70 |
| 5 | (2,1,2) | (16,8,9) | (4,2,3) | 57 |
| 6 | (4,2,3) | (16,8,9) | (2,1,2) | 56 |
| 7 | (4,2,3) | (4,2,3) | (8,4,5) | 50 |
| 8 | (16,8,9) | (2,1,2) | (4,2,3) | 57 |
| 9 | (16,8,9) | (4,2,3) | (2,1,2) | 56 |
| 10 | (32,16,17) | (2,1,2) | (2,1,2) | 70 |

Таблиця 2.

**Залежність кількості активних S-боксів від типу SPN-мережі довжиною 128 біт з трьома рівнями і розміром S-боксу — 16 біт**

| Номер варіанту | Тип КМВ нижнього рівня | Тип КМВ середнього рівня | Тип КМВ верхнього рівня | Кількість активних S-боксів |
|---|---|---|---|---|
| 1 | (2,1,2) | (2,1,2) | (16,8,9) | 45 |
| 2 | (2,1,2) | (4,2,3) | (8,4,5) | 35 |
| 3 | (2,1,2) | (8,4,5) | (4,2,3) | 33 |
| 4 | (2,1,2) | (16,8,9) | (2,1,2) | 38 |
| 5 | (4,2,3) | (2,1,2) | (8,4,5) | 35 |
| 6 | (4,2,3) | (4,2,3) | (4,2,3) | 30 |
| 7 | (8,4,5) | (2,1,2) | (4,2,3) | 33 |
| 8 | (8,4,5) | (4,2,3) | (2,1,2) | 32 |
| 9 | (16,8,9) | (2,1,2) | (2,1,2) | 38 |

Але, крім лінійного перетворення, стійкість до лінійного та диференційного криптоаналізу залежить від значення лінійної імовірності $p$ та диференційної — $q$ характеристик S-боксів. Згідно з [9] нижня межа диференційної та лінійної характеристик S-боксу розміром $n \times n$ визначається виразом:

$$q_s = p_s = \frac{n}{2^{n-1}}. \quad (7)$$

Головний показник протидії до лінійного та диференційного криптоаналізу — це імовірності лінійної $P$ та диференційної Q характеристик раундів визначається виразами [10]:

$$P = p_s^N, \quad (8)$$

$$Q = q_s^N, \quad (9)$$

де $N$ — кількість активних S-боксів.

Імовірність лінійної $P$ та диференційної $Q$ характеристик раунду, утвореного трьохрівневою гніздовою SPN мережею буде становити:

$$P = p_s^{(m_3+1)(m_1m_2+m_1+m_2+2)} = \left(\frac{n}{2^{n-1}}\right)^{(m_3+1)(m_1m_2+m_1+m_2+2)}. \quad (10)$$

Визначимо імовірності лінійної та диференційної характеристик одного раунду для гніздових трьохрівневих SPN мереж з максимальною кількістю активних S-боксів, нелінійне перетворення яких формується S-боксами розміром 8 та 16 біт.

Імовірність лінійної та диференційної характеристик раунду трьохрівневої гніздової SPN мережі з S-боксами розміром 8 біт становить:

$$P = \left(\frac{8}{2^{8-1}}\right)^{85} = (2^{-4})^{85} = 2^{-340}.$$

Імовірність лінійної та диференційної характеристик раунду трьохрівневої гніздової SPN мережі з S-боксами розміром 16 біт становить:

$$P = \left(\frac{16}{2^{16-1}}\right)^{45} = (2^{-11})^{45} = 2^{-495}.$$

По результатам обчислень очевидно, що імовірність лінійної та диференційної характеристик раунду трьохрівневих гніздових SPN мереж буде кращою у мережі, де розмір S-боксу становить 16 біт. Приклад такої SPN мережі наведено на рисунку 2.

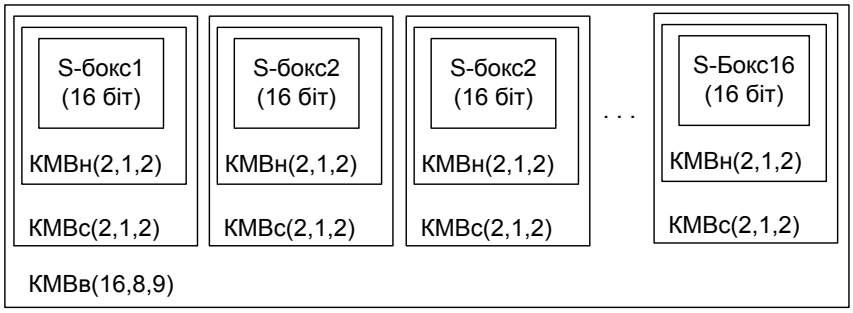


Рис. 2. Один раунд трьохрівневої гніздової SPN мережі з розміром S-боксу 16 біт

## ВИСНОВКИ

У статті запропонований метод підвищення захисту інформації в оптико-електронних системах, який базується на застосуванні блочних шифрів, що застосовують в одному раунді шифрування лінійне та нелінійне перетворення. В нелінійному перетворенні застосовуються S-бокси, розміром 16 біт. У лінійному перетворенні застосовані три рівні — нижній, середній та верхній, які об'єднані гніздовою структурою. На нижньому рівні застосовується код з максимальною відстанню типу (2,1,2), на середньому — код з максимальною відстанню типу (2,1,2) та (16,8,9) — на верхньому рівні. Проведені розрахунки демонструють, що кількість активних S-боксів такого раунду шифрування становить 45, що є в 1,8 раз більшою за кількість активних S-боксів для шифру Rijndael, який є стандартом шифрування AES, для якого цей показник становить 25 [10]. Недоліком даного раунду шифрування є необхідність застосування додаткових перетворень, що, в свою чергу, призведе до сповільнення роботи одного раунду шифрування в оптико-електронних системах. В якості подальших досліджень необхідно розробити нелінійне перетворення розміром 16 біт, яке буде мати значення лінійної та диференційної характеристик, вищі за нижню межу, яка становить $2^{-11}$.

## СПИСОК ЛІТЕРАТУРИ

1. The block cipher Hierocrypt / [Ohkuma K., Muratani H., Sano F., Kawamura S.]. // Proccedings of Selected Areas in Cryptography — SAC 2000, Lecture Notes in Computer Science, — Springer-Verlag. — 2001. — Vol, 2012. — P. 72—88.
2. Бевз О. М. Обчислювальні характеристики підстановочно-перестановочних мереж з S-боксами розміром 16×16 біт / О. М. Бевз // Оптико-електронні інформаційно-енергетичні технологіїю — 2011. — Том 21(1). — С. 9—14.
3. The cipher SHARK / [Rijmen V., Daemen J., Preneel B., Bosselaers A., Win E.] // Proceedings of Fast Software Encryption — FSE'96, Lecture Notes in Computer Science. — Springer-Verlag. — 1997. — Vol. 1039: — P. 99—112.
4. Мак-Вильямс Дж. Теория кодов, исправляющих ошибки / Мак-Вильямс Дж., Слоэн А. — М. : Связь, 1979. — 744 с.
5. Бевз О. М. Методи шифрування на основі високонелінійних бульових функцій з

максимальною відстанню: дис. … канд. техн. наук: 05.13.05 / Бевз Олександр Миколайович — Вінниця: 2008. — 181 с.
6. Бевз О. М. Визначення показників ефективності шифрування підстановочно-перестановочних мереж з блоками підстановки розміром 16×16 біт в комп'ютерних системах / О. М. Бевз, В. М. Папінов // Системи обробки інформації — 2011. — Випуск 3(93). — С. 103—106.
7. Daemen J. The Design of Rijdael. AES. The Advanced Encryption Standard / Joan Daemen, Vincent Rijman // Springer — Berlin. — 2002. — V. 234. — P. 24—28.
8. Гуц Н. Д. Алгоритмы защиты информации на основе управляемых перестановочных операций: Дис. … канд. техн. наук: 05.13.19 / Гуц Миколай Дмитриевич — СПб, 2011. —175 с.
9. O'Connor L. On the distribution of characteristics in bijective mappings / O'Connor L. / Advances in Cryptology — EUROCRYPT'93. — Springer-Verlag. 1994. — Vol. 678. — P. 360—370.
10. Kanda M. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function. / M. Kanda // Seventh Annual International Workshop on Selected Areas in Cryptography — SAC'00, Lecture Notes in Computer Science — Springer-Verlag, 2001. — Vol. 2012. — P. 324—338.

Надійшла до редакції 16.10.2014 р.

**БЕВЗ ОЛЕКСАНДР МИКОЛАЙОВИЧ — к. т. н, доцент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.**

**ЯРОВЕНКО АНАСТАСІЯ ОЛЕКСІЇВНА — студентка гр. 1КСУА-14м кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.**