[12]. Lai X., Massey J.L. A proposal for a new block encryption standard //Advances in Cryptology – Proc. Eurocrypt'90, LNCS 473, Springer–Verlag, 1991, pp. 389–404
[13]. Lai X., Massey J.L. On the design and security of block cipher //ETH series in information processing, v.1, Konstanz: Hartung–Gorre Verlag, 1992.

ПРО МЕРЕЖІ RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 ТА RFWKPES16–1, СТВОРЕНІ НА ОСНОВІ МЕРЕЖІ PES16–8

У статті на осное мережі PES16–8 розроблені мережі RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 і RFWKPES16–1 складаються з восьми, чотирьох, двох і однієї раундових функцій. Основна перевага запропонованих мереж в тому, що при зашифрованих і расшифровании використовується один і той же алгоритм, а також як раундових функцій можна використовувати будь– які перетворення. В розроблених мережах довжина подблоков дорівнює 8, 16 і 32 бітам і на основі цієї мережі можна створити алгоритм шифрування довжиною блоку 128, 256 і 512 бітам. Крім цього, алгебраїчні операції є змінними, в якості цих операції можна використовувати операції додавання і множення по модулю і XOR.
Ключові слова: мережа Фейстеля, схема Лай–Мессі, раундова функція, зашифрование, розшифрування, мультиплікативна інверсія, аддитивная інверсія.

ABOUT NETWORKS RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 AND RFWKPES16–1, CREATED ON THE BASIS NETWORK PES16–8

In the paper on the basis of the network PES16–8 developed networks RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 and RFWKPES16–1 consisting of eight, four, two, and one round function. The main advantage of the proposed network that during encryption and decryption using the same algorithm as well as a round function can be any transformation. In the network PES16-8 length of subblock is 8, 16 and 32 bits and basis on the network can create the encryption algorithm a length of subblock 128, 256 and 512 bits. In a network PES16-8 algebraic operations are variable, as these operations can use the operations of addition and multiplication modulo and XOR
Index terms: Feistel network, Lai–Massey scheme, round function, encryption, decryption, multiplicative inverse, additive inverse.

Туйчиев Гулом Нумонович, кандидат технических наук, преподаватель Национального университета Узбекистана.
E-mail: blasterjon@gmail.com
Туйчієв Гулом Нумович, кандидат технічних наук, викладач Національного університета Узбекистана.
Tuychiev Gulom, PhD, Assossiate Professor, National university of Uzbekistan.

УДК 004.027

МЕТОДИ ШИФРУВАННЯ НА ОСНОВІ ПЕРЕСТАНОВКИ БЛОКІВ ЗМІННОЇ ДОВЖИНИ

Володимир Лужецький, Іван Горбенко

Однією з основних операцій, яка використовується в багатьох блокових шифрах, є перестановка. Сучасні блокові шифри здійснюють операцію перестановки лише в межах окремого блоку або невеликої групи блоків. В одній з попередній публікацій було запропоновано метод псевдовипадкової перестановки блоків в межах усього повідомлення, однак у сучасних шифрах довжина блоку є фіксованою, тому, навіть після перестановки блоків, початкові та кінцеві позиції блоків залишаються відомими. Для підвищення криптографічної стійкості запропоновано здійснювати розбиття повідомлення на блоки змінної довжини. Розроблено методи шифрування на основі перестановки блоків змінної довжини, сформовано рекомендації стосовно кількості можливих значень довжини блоку та діапазону цих значень, запропоновано правила формування псевдовипадкових значень довжин блоків, наведено їх порівняння з точки зору забезпечення стійкості.
Ключові слова: *перестановка, блоки змінної довжини, відкрите повідомлення, шифротекст, генератор псевдовипадкових чисел.*

Вступ. Відомо [1], що перестановка є однією з базових (разом з підстановкою) операцій алгоритмів шифрування. Зокрема, операція перестановки використовується у сучасних архітектурах блокових шифрів (таких як мережа Фейстеля, SP-мережа, "квадрат"). Однак, ці архітектури передбачають здійснення перестановки частин окремого блоку або перестановки блоків в межах невеликої групи. Так, мережа Фейстеля передбачає розбиття блоку даних на дві або чотири частини і здійснення фіксованої перестановки цих частин [2]. SP-мережа здійснює перестановку чотирьох і

більше елементів, але також в межах окремого блоку [3]. Для архітектури "квадрат" перестановка має специфіку, оскільки дані представляються у вигляді матриць, однак теж переставляються лише частини окремого блоку [4].

Крім того, перестановка, яку виконують відомі методи шифрування, є фіксованою (не залежить від ключа). Отже, можливість підвищення криптографічної стійкості за рахунок перестановки використовується не повною мірою.

У [5] запропоновано метод формування правил перестановок, який дозволяє здійснювати псевдовипадкову (залежну від секретного ключа) перестановку блоків в межах всього повідомлення, що дозволяє в більшому обсязі використовувати можливості операції перестановки.

Однак, сучасні блокові шифри передбачають розбиття повідомлення на блоки фіксованої довжини. Оскільки довжина блоку та обсяг повідомлення є відкритими, то відомою є кількість блоків, а також, що більш суттєво, початкова і кінцева позиції кожного з блоків. Ці значення не змінюються навіть після перестановки блоків, а отже, зловмисник має можливість здійснювати дешифрування окремого блоку. Таким чином, перестановка блоків фіксованої довжини, навіть в межах усього повідомлення, не забезпечує максимальної криптографічної стійкості.

Метою дослідження є підвищення криптографічної стійкості шифру на основі перестановки блоків.

Для досягнення мети дослідження потрібно розв'язати такі задачі:

1. Розробити метод шифрування на основі перестановки блоків змінної довжини.

2. Розробити метод розбиття повідомлення на блоки, при перестановці яких початкові та кінцеві позиції блоків змінюються.

Отримати оцінки методу з точки зору криптографічної стійкості та витрат ресурсів.

Методи шифрування. Пропонується метод шифрування на основі перестановки блоків, особливість якого полягає в тому, що перестановці підлягають блоки змінної довжини в межах усього повідомлення. Алгоритм перестановки блоків змінної довжини полягає в такому. Нехай повідомлення M розбите на N блоків:

$$M = \{m_0 \parallel m_1 \parallel ... \parallel m_{N-1}\}.$$

Передбачається виконання двох основних операцій: зчитування блоків відкритого повідомлення та запис блоків шифротексту. Зчитування та запис блоків можуть здійснюватись у природному порядку (від 0-го до (N – 1)-го блоку з кроком один):

$$m_0, m_1, m_2, ..., m_{N-2}, m_{N-1},$$

у детермінованому, тобто згідно з певним правилом, або у псевдовипадковому. Нехай операція зчитування позначається літерою R, операція запису – літерою W. Таким чином, узагальнений метод шифрування Cf позначається так:

$$Cf = (R, W)$$

Нехай зчитування або запис у природному порядку умовно позначається літерою U, у детермінованому – літерою D, а у псевдовипадковому порядку – літерою P.

Метод $Cf = (R_U, W_D)$ передбачає зчитування блоків вихідного повідомлення в природному порядку. Формування шифротексту починається з 0-го блоку відкритого повідомлення. Таким чином, початковий шифротекст має вигляд:

$$C_0 := m_0.$$

Всі наступні блоки з непарними індексами дописуються до початку повідомлення, а всі блоки з парними індексами – до кінця повідомлення. Тобто на кожному кроці поточний шифротекст C_i матиме вигляд:

$$C_i = \begin{cases} C_{i-1} \parallel m_i, \text{ якщо } i \text{ парне;} \\ m_i \parallel C_{i-1}, \text{ якщо } i \text{ непарне.} \end{cases} \quad (1)$$

Таким чином, порядок блоків у шифротексті C матиме вигляд:

$$C = m_{N-1} \parallel m_{N-3} \parallel ... \parallel m_3 \parallel m_1 \parallel m_0 \parallel m_2 \parallel m_4 \parallel ... \parallel m_{N-4} \parallel m_{N-2}.$$

Метод $Cf = (R_D, W_U)$ передбачає почергове зчитування блоків відкритого повідомлення – з початку та з кінця повідомлення, а запис блоків шифротексту – у природному порядку. Тобто правило формування шифротексту описується формулою:

$$C_i := C_{i-1} \parallel m_j,$$

а значення індексу j визначається за правилом:

$$j = \begin{cases} \dfrac{i}{2}, & \text{якщо } i \text{ парне,} \\ N - \dfrac{i+1}{2}, & \text{якщо } i \text{ непарне.} \end{cases} \quad (2)$$

Тобто порядок блоків після перестановки має вигляд:

$$C = m_0 \parallel m_{N-1} \parallel m_1 \parallel m_{N-2} \parallel ... \parallel m_{\frac{N-1}{2}}.$$

При такому підході однією із задач є визначення початкових позицій блоків відкритого повідомлення, які зчитуються для формування шифротексту. Нехай відкрите повідомлення складається з L байтів. Так, на початку формування шифротексту, початкова позиція першого блоку

дорівнює 0, а останнього $L-l(m)$, де $l(m)$ – довжина останнього блоку в байтах. На кожному кроці, після зчитування блоку відкритого повідомлення, значення початкових позицій змінюються. Для спрощення процедури визначення початкових позицій блоків, пропонується кожен використаний блок вилучати з відкритого повідомлення. Тоді на кожному кроці потрібно буде зчитувати або перший або останній блок. На кожному кроці після вилучення одного блоку залишкова довжина повідомлення дорівнює $L-l(m_i)$. Тоді початкова позиція першого блоку завжди дорівнюватиме 0, а останнього $L-l(m)$.

Однак, обидва підходи забезпечують детермінований порядок розташування блоків після перестановки, а тому криптографічна стійкість шифру на основі такої перестановки визначається лише правилом вибору довжин блоків. Детермінованість порядку пов'язана з тим, що ознакою визначення адреси запису блоку шифротексту (у першому варіанті) або адреси зчитування блоку відкритого повідомлення (у другому варіанті) є індекс блоку відкритого повідомлення. Тому для забезпечення псевдовипадкового порядку блоків після перестановки пропонується ввести певне правило формування відповідної ознаки. Для формування такої ознаки може бути використаний генератор на основі регістра зсуву зі зворотним зв'язком (РЗЗЗ). На кожному кроці зчитується значення s_i виходу генератора:

$$s_i = \{0,1\},$$

яке використовується в якості ознаки.

Так, у методі $Cf = (R_U, W_P)$ якщо $s_i = 0$, то формування нового шифротексту відбувається шляхом дописування наступного блоку відкритого повідомлення до початку попереднього шифротексту, а якщо $s_i = 1$, тоді блок відкритого повідомлення дописується до кінця попереднього шифротексту:

$$C_i = \begin{cases} C_{i-1} \,||\, m_i, \text{ якщо } s_i = 0; \\ m_i \,||\, C_{i-1}, \text{ якщо } s_i = 1. \end{cases} \quad (3)$$

У методі $Cf = (R_P, W_U)$, якщо $s_i = 0$, то формування нового шифротексту відбувається шляхом додавання до попереднього шифротексту блоку з початку відкритого повідомлення, а якщо $s_i = 1$ – блоку з кінця відкритого повідомлення:

$$j = \begin{cases} \dfrac{i}{2}, & \text{якщо } s_i = 0; \\ N - \dfrac{i+1}{2}, & \text{якщо } s_i = 1. \end{cases} \quad (4)$$

Можливі варіанти побудови шифру з використанням формул (1) – (4) наведені у табл. 1.

Методи розбиття повідомлення на блоки

Для вирішення задач дослідження потрібно виконати такі дії:

1) обрати діапазон та набір значень довжини блоків;

2) сформувати правило вибору цих значень.

Однією із задач є вибір кількості можливих значень довжини блоку. Недостатня кількість не забезпечує належної криптографічної стійкості. Надмірна кількість ускладнює процес шифрування. Крім того, використання великої кількості значень призведе до появи блоків великих розмірів, а отже – появи монотонності після перестановки блоків.

Оскільки значення довжин блоків можуть бути випадковими, то доцільно кожному з них присвоїти код – порядковий номер, починаючи з 0, та здійснювати вибір значень довжин блоків на основі таких кодів.

Вибір значень довжин блоків може бути детермінованим або псевдовипадковим. При детермінованому виборі значення формуються згідно з певним правилом. Цей варіант має свої недоліки. По-перше, початкові та кінцеві позиції блоків залишаються відомими. Вони будуть змінені після перестановки блоків, а тому такий варіант доцільно використовувати лише у поєднанні з подальшою псевдовипадковою перестановкою усіх блоків повідомлення. По-друге, при такому підході період послідовності значень дорівнює кількості можливих значень блоків Q. Оскільки це значення, в більшості випадків, набагато менше кількості блоків N, на яку розбите повідомлення, матимуть місце повторення

$$T = Q; \quad T << N.$$

Отже, для забезпечення криптографічної стійкості доцільно використовувати псевдовипадковий порядок вибору значень довжин блоків. Для цього пропонуються такі варіанти.

Нехай кількість значень довжини блоків Q. Отже генератор повинен формувати значення в діапазоні $[0; Q-1]$.

Таблиця 1

Можливі варіанти побудови шифру

Метод шифрування	**Правило формування шифротексту**
$Cf = (R_U W_D)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_i, \text{ якщо } i \text{ парне;} \\ m_i \,\|\| \, C_{i-1}, \text{ якщо } i \text{ непарне.} \end{cases}$
$Cf = (R_D W_U)$	$C_i := C_{i-1} \,\|\| \, m_j$, де $j = \begin{cases} \dfrac{i}{2}, & \text{якщо } i \text{ парне;} \\ N - \dfrac{i+1}{2}, & \text{якщо } i \text{ непарне.} \end{cases}$
$Cf = (R_U W_P)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_i, \text{ якщо } s_i = 0; \\ m_i \,\|\| \, C_{i-1}, \text{ якщо } s_i = 1; \end{cases}$
$Cf = (R_P W_U)$	$C_i := C_{i-1} \,\|\| \, m_j$, де $j = \begin{cases} \dfrac{i}{2}, & \text{якщо } i \text{ парне;} \\ N - \dfrac{i+1}{2}, & \text{якщо } i \text{ непарне.} \end{cases}$
$Cf = (R_D W_D)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_j, \text{ якщо } i \text{ парне,} \\ m_j \,\|\| \, C_{i-1}, \text{ якщо } i \text{ непарне,} \end{cases} \quad j = \begin{cases} \dfrac{i}{2}, \text{ якщо } i \text{ парне;} \\ N - \dfrac{i+1}{2}, \text{ якщо } i \text{ непарне.} \end{cases}$
$Cf = (R_D W_P)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_j, \text{ якщо } i \text{ парне;} \\ m_j \,\|\| \, C_{i-1}, \text{ якщо } i \text{ непарне;} \end{cases} \quad j = \begin{cases} \dfrac{i}{2}, & \text{якщо } s_i = 0; \\ N - \dfrac{i+1}{2}, & \text{якщо } s_i = 1; \end{cases}$
$Cf = (R_P W_D)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_j, \text{ якщо } s_i = 0; \\ m_j \,\|\| \, C_{i-1}, \text{ якщо } s_i = 1; \end{cases} \quad j = \begin{cases} \dfrac{i}{2}, & \text{якщо } i \text{ парне;} \\ N - \dfrac{i+1}{2}, & \text{якщо } i \text{ непарне;} \end{cases}$
$Cf = (R_P W_P)$	$C_i = \begin{cases} C_{i-1} \,\|\| \, m_j, \text{ якщо } s_i = 0; \\ m_j \,\|\| \, C_{i-1}, \text{ якщо } s_i = 1; \end{cases} \quad j = \begin{cases} \dfrac{i}{2}, & \text{якщо } s_i = 0; \\ N - \dfrac{i+1}{2}, & \text{якщо } s_i = 1. \end{cases}$

Одним із недоліків такого генератора є необхідність виконання операції множення, яка є складною для мікропроцесорної техніки. Однак, що більш суттєво, період такого генератора при застосуванні для вирішення даної задачі, дорівнює кількості можливих значень Q довжини блоків. Тобто використання цього генератора має такий самий недолік, як і використання детермінованого порядку вибору значень довжини блоків.

Генератор на основі регістра зсуву зі зворотним зв'язком є простим у реалізації та має високу швидкість. Цей генератор формує послідовність двійкових символів. Таким чином, кількість можливих послідовностей з k символів складає 2^k. Отже, якщо кількість можливих значень довжини блоку є степенем двійки ($Q = 2^k$), то кожній послідовності з k символів ставиться у відповідність один код значення довжини блоку. Тому доцільно обирати саме таке значення Q. Якщо значення Q не є степенем двійки, тоді потрібно обрати мінімальну довжину k послідовності двійкових символів, за допомогою якої можна закодувати Q значень:

$$k = \left] \log_2 Q \right[+ 1.$$

В такому випадку не кожна послідовність довжиною k символів відповідатиме коду значення довжини блоку. Отже при виборі послідовностей з k двійкових символів $2^k - Q$ таких послідовностей не братимуть участі у формуванні кодів значень довжин блоків, а тому не повною мірою використовується можливість такого методу генерування. Підхід, який усуває вказаний недолік, полягає в тому, що кожній з 2^k послідовностей ставиться у відповідність число за рахунок повто-

рного використання $2^k - Q$ чисел. Але недоліком цього підходу є неоднакова імовірність вибору того чи іншого числа, на основі якого формується код значення довжини блоку.

Можливі такі варіанти використання генератора на основі РЗЗЗ для вирішення поставленої задачі. Один із варіантів полягає в такому. Генератор на основі РЗЗЗ формує послідовність бітів:

$$P = p_0, p_1, p_2, \ldots, \text{ де } p_i = \{0,1\}.$$

Для формування кодів значень довжин блоків із цієї послідовності почергово вибираються групи з k послідовних символів:

$$g_0 = \{p_0, p_1, \ldots, p_{k-1}\},\ g_1 = \{p_k, p_{k+1}, \ldots, p_{2k-1}\},\ \text{і т.д.}$$

Кожній такій групі, згідно з певним правилом, ставиться у відповідність число, яке і визначає код значення довжини блоку:

$$l_i = \sum_{j=0}^{k-1} g_{i,j} \cdot 2^j .$$

У випадку, якщо значення Q не є степенем 2, за вказаною формулою визначається допоміжний параметр x_i:

$$x_i = \sum_{j=0}^{k-1} g_{i,j} \cdot 2^j .$$

Якщо $x_i < Q$, тоді код значення довжини блоку l_i дорівнює значенню x_i:

$$l_i = x_i,$$

інакше або поточне значення x_i не використовується і формується наступне значення, або код значення довжини блоку визначається так:

$$l_i = x_i - Q.$$

Інший варіант передбачає формування кодів значень довжини блоку на основі станів генератора РЗЗЗ. Однак, аналізується не вихід генератора, а його стан S_i з d розрядів, який розглядається як число:

$$S_i = \{s_{i,j}\},\ j = 0,1,\ldots,d-1.$$

Алгоритм полягає в такому. Зі стану генератора обирається група з k молодших розрядів:

$$g_i = \{s_{i,(d-k+1)}, s_{i,(d-k+2)}, s_{i,(d-1)}\},$$

на основі якої, аналогічно до попереднього варіанту, формується код значення довжини блоку l_i.

Після цього обирається група з наступних k розрядів. Таким чином, якщо d кратне k, на основі одного стану генератора буде сформовано $\frac{d}{k}$ кодів значень довжини блоку, після чого відбувається формування нового стану генератора. Якщо d не кратне k, тоді на основі одного стану формується $\left]\frac{d}{k}\right[$ кодів значень довжини блоку, а залишкова кількість розрядів складає:

$$r = d - \left]\frac{d}{k}\right[.$$

Потім формується новий стан генератора s_{i+1}. З нього обирається $(k - r)$ молодших розрядів, які об'єднуються із залишковими r розрядами з попереднього стану:

$$g_i = \{s_{(i+1),(d-r+1)}, \ldots, s_{(i+1),(d-1)}, s_{i,0}, \ldots, s_{i,(r-1)}\}.$$

Приклад вибору двійкових розрядів зі станів генератора наведено на рис. 1.

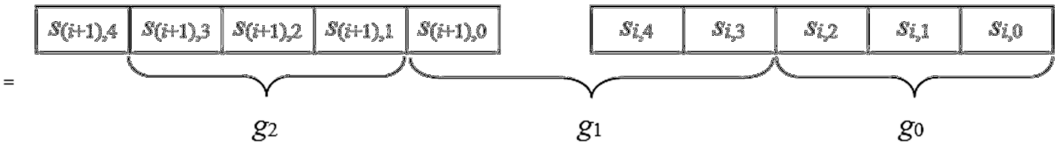

Рис. 1. Приклад вибору розрядів зі станів генератора

Після цього, вибір груп з k розрядів із нового стану відбувається звичайним чином.

Розглянемо період кожного із запропонованих генераторів значень довжини блоку. У першому варіанті використовується генератор ПВП на основі РЗЗЗ розрядністю d, отже його період складає:

$$T_0 = 2^d - 1.$$

Для формування одного значення довжини блоку обирається k розрядів. Отже, період складає:

$$T_1 = \frac{HCK(k, T_0)}{k}.$$

Для забезпечення максимального значення періоду значення k та T_0 повинні бути взаємно простими. Тоді період складе:

$$T_1 = \frac{k \cdot T_0}{k} = T_0 = 2^d - 1.$$

Оскільки у другому варіанті використовуються стани генератора, а для формування окремих кодів значень довжини блоку можуть використовуватися розряди двох суміжних станів, то період в такому випадку визначається як найменше спільне кратне періоду T_0 генератора на основі РЗЗЗ та значення k:

$$T_2 = HCK(T_0, k).$$

Якщо T_0 та k – взаємно прості числа, період складає:

$$T_2 = T_0 \cdot k = (2^d - 1) \cdot k .$$

Таким чином, для забезпечення більшого періоду, а отже – вищої криптографічної стійкості, доцільніше використовувати другий варіант правил вибору значень довжини блоків, за умови, що кількість розрядів d генератора на основі РЗЗЗ та значення періоду не кратні кількості розрядів k.

Висновки. Всі відомі блокові шифри виконують операцію перестановки лише в межах окремого блоку або невеликої групи блоків. Причому довжина блоку є фіксованою, отже навіть за умови здійснення перестановки блоків у межах всього повідомлення, початкові та кінцеві позиції блоків залишаються відомими.

Для підвищення стійкості шифру на основі перестановки блоків запропоновано здійснювати розбиття повідомлення на блоки змінної довжини. Для цього запропоновано метод шифрування на основі перестановки блоків змінної довжини, сформовано рекомендації щодо кількості можливих значень довжини блоку та діапазону цих значень, а також запропоновано метод формування псевдовипадкових значень довжини блоку.

Було розглянуто декілька можливих варіантів реалізації розробленого методу та проведено порівняння цих варіантів з точки зору криптографічної стійкості, яку вони забезпечують, та з точки зору швидкості роботи та апаратних витрат, на основі отриманих оцінок обрано найбільш прийнятний варіант.

ЛИТЕРАТУРА

[1]. Шеннон К. Работы по теории информации и кибернетике. — М.: Изд. иностр. лит., 1963. — 830 с.

[2]. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002 – 816 с.

[3]. Ковалевский В. Криптографические методы. – М.: "Компьютер Пресс", 1993 – 236 с.

[4]. Баричев С. Г., Гончаров В. В. Стандарт AES. Алгоритм Rijndael. – М.: "Горячая линия – Телеком", 2002 – с. 30 – 35.

[5]. Лужецький В.А. Метод формування перестановок довільної кількості елементів / В.А.Лужецький, І.С.Горбенко // Захист інформації. – 2013. – №3 – С. 262-267.

[6]. Кнут Д. Искусство программирования. Часть 2. – М.: "Мир", 1976 – 788 с.

REFERENCES

[1]. Shannon, Works on information theory and cybernetics., M: Publishing House. foreign. Lighted., 1963, 830 p.

[2]. B. Schneier, Applied Cryptography, M: Triumph, 2002, 816 p.

[3]. Kovalevsky V. cryptographic methods, M .: "Computer Press", 1993, 236 p.

[4]. Barichev SG, Goncharov VV Standard AES. The algorithm Rijndael, M: "Hot Line-Telecom", 2002, p. 30-35.

[5]. Luzhetsky V.A., Gorbenko I.S. Method formuvannya permutations dovilnoї kilkosti elementiv, Zahist Informácie, 2013, №3, p. 262-267.

[6]. Knuth Art of Computer Programming. Part 2, M: "The World", 1976, 788 p.

МЕТОДЫ ШИФРОВАНИЯ НА ОСНОВЕ ПЕРЕСТАНОВКИ БЛОКОВ ПЕРЕМЕННОЙ ДЛИНЫ

Одной из основных операций, которую выполняют блоковые шифры, независимо от их архитектуры, является перестановка. Современные блоковые шифры осуществляют операцию перестановки только в пределах отдельного блока или небольшой группы блоков. В одной из предыдущих публикаций был предложен метод псевдослучайной перестановки блоков в пределах всего сообщения, однако в современных шифрах длина блока является фиксированной, потому, даже после перестановки блоков, начальные и конечные позиции блоков остаются известными. Для повышения криптографической стойкости предлагается осуществлять разбиение сообщения на блоки переменной длины. Разработано методы шифрования на основании перестановки блоков переменной длины, сформировано рекомендации относительно количества возможных значений длины блока и диапазона этих значений, предложено правила формирования псевдослучайных значений длин блоков, приведено их сравнения с точки зрения обеспечения стойкости.

Ключевые слова: перестановка, блоки переменной длины, открытое сообщение, шифротекст, генератор псевдослучайных чисел.

METHODS OF ENCRYPTION BASED ON PERMUTATION UNITS WITH VARIABLE LENGTH

One of the main operations performed by the block ciphers regardless to their architecture is permutation. Modern block ciphers perform permutation operation only inside a separate block or small group of blocks. In one of the previous articles the method of pseudorandom permutation of blocks inside the entire message was offered but modern block ciphers have fixed block length so even after permutation the beginning and ending blocks positions remain known. To increase the cryptographic strength fragmentation the message to variable length blocks is offered. Ciphering methods based on variable length blocks permutation were developed, recommendations concerning blocks length quantity and their range were produced, the rules of pseudorandom blocks length values generating were offered and com-

pared from cryptographic strength providing point of view.
Index terms: permutation, variable length blocks, open message, ciphertext, pseudorandom numbers generator.

Лужецький Володимир Андрійович, доктор технічних наук, професор, завідувач кафедри захисту інформації, Вінницький національний технічний університет.
E-mail: lva_zi@mail.ru.
Лужецкий Владимир Андреевич, доктор технических наук, профессор, заведующий кафедрой защиты информации, Винницкий национальный технический университет.
Luzhetsky Volodymyr, Doctor of Technical Sciences, Professor, Head of Information Security Academic Departmant, Vinnytsia National Technical University.

Горбенко Іван Сергійович, аспірант кафедри захисту інформації, Вінницький національний технічний університет.
E-mail: milyaga89@gmail.com.
Горбенко Иван Сергеевич, аспирант кафедры защиты информации, Винницкий национальный технический университет.
Gorbenko Ivan, postgraduate student Information Security Academic Departmant, Vinnytsia National Technical University.

УДК 004.056.53:004.492.3 (045)

МЕТОД ВИЯВЛЕННЯ ІНЦИДЕНТІВ/ПОТЕНЦІЙНИХ КРИЗОВИХ СИТУАЦІЙ

Микола Карпінський, Анна Корченко, Андрій Гізун

Розвиток інформаційних технологій призвів до збільшення залежності людського суспільства від них і різкого зростання інцидентів інформаційної безпеки, що за умов відсутності контролю за ними можуть спричиняти кризові ситуації. Чим вищий рівень критичності інциденту/потенційної кризової ситуації, тим серйозніші збитки він здатен завдати і тому вимагає значно серйознішого захисту. Одним з основних аспектів, який визначає ефективність захисту, є автоматизація і своєчасність виявлення та ідентифікації інцидентів. В роботі запропонований метод виявлення інцидентів/потенційних кризових ситуацій, що базується на застосуванні теорії нечітких множин та експертних підходів. Оскільки процеси в інформаційних системах характеризуються певним рівнем невизначеності та випадковості і носять нечіткий характер, то такий метод може бути використаний для реалізації задач захисту інформації. Складається метод з 6 етапів: формування множин інцидентів/потенційних кризових ситуацій та ідентифікуючих параметрів; формування зв'язки інцидент – набір нечітких ідентифікуючих параметрів; формування еталонів нечітких параметрів; формування наборів евристичних правил для виявлення та ідентифікації інцидентів; фазифікації параметрів, що моніторяться для виявлення інциденту; обробки параметрів та формування результату. Запропонований метод може застосовуватися окрема або в комплексі з методом оцінки рівня критичності ситуації, що склалася внаслідок впливу інциденту/потенційної кризової ситуації.
***Ключові слова**: кризова ситуація, інцидент, рівень критичності кризової ситуації, експертні методи, теорія нечітких множин, виявлення та ідентифікація кризових ситуацій, інтегрована модель.*

Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми так і на засоби для проведення інформаційних атак, набір можливих інцидентів/потенційних кризових ситуацій (ІПКС) значно збільшується. Безперервно зростає кількість загроз інформаційній безпеці, проводяться нові кібератаки на інформаційні ресурси (ІР), що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ІР можливе за умови обізнаності щодо можливих ІПКС, що створює передумови для підбору та застосування найбільш адекватних заходів та засобів захисту. Крім того, задачі прийняття рішень в умовах КС потребують значних часових та виробничих ресурсів, а також встановлення додаткових вимоги до особи, що приймає рішення, з точки зору швидкості її реакції та вміння оцінити поточне становище. Дана задача ускладнюється тим, що атаки на ІР здійснюються в реальних умовах, тобто з великим показником випадковості та непередбачуваності. Виходячи з цього дуже складно оперувати статистичними даними, які використовуються в класичних методах та засобах управління КС. Дану проблему може вирішити застосування методів та математичного апарату нечіткої логіки, ефективність застосування яких для вирішення задач, пов'язаних з забезпеченням інформаційної безпеки, показана в роботі [1]. Тому розробка методу виявлення ІПКС є актуальною задачею.