УДК 004.056.55:519.2

С. Яковлєв
НТУУ “КПІ”, Фізико-технічний інститут,
кафедра математичних методів захисту інформації

ДОКАЗОВА ТА ПРАКТИЧНА СТІЙКІСТЬ R-СХЕМИ БЛОЧНОГО ШИФРУВАННЯ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

Наведено аналітичні оцінки верхніх меж імовірностей існування нетривіальних диференціалів та диференціальних характеристик для немарковської R-схеми блочного шифрування.

Ключові слова: симетричні блочні шифри, диференціальний аналіз, схема Фейстеля, R-схема.

Upper bounds for differential probabilities and differential characteristic probabilities of non-Markov R-scheme are estimated.

Key words: symmetric block ciphers, differential analysis scheme Feystelya, R-scheme.

Вступ

Схема Фейстеля є однією з класичних схем синтезування алгоритмів блочного шифрування [1]. Їй притаманні простота, зручність та менша вибагливість до обчислювальних ресурсів порівняно з підстановково-перестановковими мережами; окрім того, оскільки американський стандарт шифрування DES побудовано за схемою Фейстеля, вона є добре вивченою та детально дослідженою. Різні дослідники розробляли модифікації схеми Фейстеля, що зберігали плюси та надавали ті чи інші додаткові переваги. Наприклад, японський криптограф М. Мацуі запропонував так звану MISTY-схему (або L-схему) [2], що піддавалась паралелізації під час обчислення; цю схему покладено в основу шифрів сімейства MISTY. Коли ж виявилось, що L-схема вразливіша до деяких суто теоретичних атак, ніж оригінальна схема Фейстеля, було запропоновано іншу модифікацію – R-схему [3, 10], яку проаналізовано у цій роботі.

Диференціальний аналіз є одним з найпотужніших сучасних засобів криптоаналізу симетричних блочних шифрів. У перших відкритих публікаціях з диференціального аналізу (Е. Біхам, А. Шамір, 1991–1992 рр. [4, 5]), розглянуто застосування цього виду атак до шифрів DES та FEAL, і продемонстровано його неординарну потужність. Надалі вимога стійкості до диференціального аналізу та різних його модифікацій стала однією з необхідних під час синтезування новітніх алгоритмів шифрування.

Задачу доказової стійкості схеми шифрування до диференціального аналізу сформулювали К. Ніберг та Л.Р. Кнудсен у 1994 р. [8]; вони одержали верхню межу імовірності існування нетривіальних диференціалів DES-подібної схеми Фейстеля. Результати Ніберг та Кнудсена поліпшили Аокі та Ота [9] для випадку, коли як раундові перетворення DES-подібної схеми Фейстеля використовуються бієктивні функції. М. Мацуі навів аналогічні оцінки для L-схеми [2], а Канеко, Сано та Сакураі – для R-схеми (і для деяких інших модифікацій схеми Фейстеля) [10]. Також, вслід за Кнудсеном [12] та Кандою [13], почали розрізняти *теоретичну* (доказову) та *практичну* стійкість до диференціального аналізу; перша стосується оцінки імовірностей існування диференціалів, друга – диференціальних характеристик.

Однак необхідно зауважити, що всі згадані результати стосувались саме DES-подібних шифрів, а у ширшому розумінні – алгоритмів, що належать класу так званих *марковських шифрів* [6, 7]. Властивості марковських шифрів значно спрощують аналіз та оцінювання стійкості до

диференціальних атак; для немарковських шифрів ці властивості не виконуються, а тому в загальному випадку не будуть коректними результати, одержані для марковських шифрів.

Теоретичні дослідження немарковських схем шифрування, зокрема, ГОСТ-подібних шифрів, наведено в серії робіт Л.В. Ковальчук [14–16]. Зокрема, нею одержані оцінки верхніх меж існування нетривіальних диференціалів для немарковських схеми Фейстеля та L-схеми, аналогічні оцінкам Аокі, Оти та Мацуі. У цій роботі ми продовжуємо цей напрям. Нами будуть наведені точніші оцінки для диференціальних імовірностей немарковської R-схеми, які визначають доказову стійкість до диференціального аналізу, а також оцінки для імовірностей диференціальних характеристик R-схем, які визначають практичну стійкість. Дані оцінки виявились справедливими і для двох інших схем.

У першому розділі статті наведено формальний опис ітеративного блочного шифру, схеми Фейстеля, L-схеми та R-схеми, а також введено інші необхідні терміни та позначення. Другий розділ присвячено основним теоретичним положенням диференціального криптоаналізу. В третьому розділі ми коротко формулюємо існуючі та отримані результати, виводимо оцінки стійкості немарковської R-схеми до диференціального криптоаналізу.

1. Необхідні терміни та визначення

У цьому розділі ми наведемо визначення ітеративного симетричного блочного шифру та інші необхідні означення.

Раундове перетворення F_k – перетворення виду $F_k : V_q \times K \to V_q$, де V_q – множина бітових векторів довжини q, K – множина раундових ключів (ключовий простір) та $k \in K$. Ми будемо також вживати термін *раунд шифрування*, або просто *раунд*, маючи на увазі раундове перетворення.

Якщо раундове перетворення за структурою лінійно виражається через деяку іншу (нелінійну) функцію f_k меншої розмірності, то таку функцію ми називатимемо *раундовою функцією*.

Ітеративний r-раундовий блочний шифр E – перетворення виду $E : V_q \times K^r \to V_q$, що є композицією r раундових перетворень: $E = F_{k_r}^{(r)} \circ F_{k_{r-1}}^{(r-1)} \circ ... \circ F_{k_1}^{(1)}$. Зауважимо, що тут і надалі ми вважаємо, що раундові ключі $(k_1, k_2, ..., k_r)$ є випадковими, незалежними та рівномірно розподіленими в ключовому просторі.

Якщо $Y = E_k(X)$, то будемо розглядати пов'язану із шифром послідовність $(X_0, X_1, ..., X_r)$, де $X_0 = X$, $X_i = F_{k_i}^{(i)}(X_{i-1})$, $Y = X_r$.

Підхід, запропонований Хорстом Фейстелем для побудови блочних шифрів [1], полягав у тому, що на кожному раунді шифрування виконуються відносно прості математичні перетворення, а необхідний рівень стійкості забезпечується достатньо великою кількістю раундів та різними ключами на кожному раунді. Зокрема, Фейстель запропонував розбивати вхідний блок навпіл та опрацьовувати на кожному раунді лише половину блоку, змішуючи її наприкінці з іншою половиною; в цьому випадку, наприклад, 64-бітові блочні шифри можуть бути ефективно реалізовані на 32-бітній архітектурі.

Схема Фейстеля – ітеративний блочний шифр, кожен раунд шифрування якого має таку структуру:

$$F_k : (V_n)^2 \times K \to (V_n)^2,$$
$$F_k(x, y) = (y, x \oplus f_k(y)),$$

де f_k – відповідна раундова функція, а $\oplus$ – операція побітового додавання двійкових векторів (XOR). Схему Фейстеля із r раундів, на яких використовуються раундові функції $f_k^{(1)}$, $f_k^{(2)}, ..., f_k^{(r)}$, традиційно позначають через $\Psi[f_k^{(1)}, f_k^{(2)}, ..., f_k^{(r)}]$.

L- та R-схеми визначаються так само, як і схема Фейстеля, відмінність полягає лише у структурі раундового перетворення.

MISTY-схема (або *L-схема*) – ітеративний блочний шифр, кожен раунд шифрування якого має таку структуру:

$$F_k(x, y) = (y,\ y \oplus f_k(x)).$$

R-схема – ітеративний блочний шифр, кожен раунд шифрування якого має таку структуру:

$$F_k(x, y) = (y \oplus f_k(x),\ f_k(x)).$$

За аналогією ми будемо використовувати позначення $L[f_k^{(1)}, f_k^{(2)}, ..., f_k^{(r)}]$ та $R[f_k^{(1)}, f_k^{(2)}, ..., f_k^{(r)}]$ для L- та R-схеми із r раундів, на яких використовуються раундові функції $f_k^{(1)},\ f_k^{(2)}, \ldots, f_k^{(r)}$.

Наведемо ще одне необхідне нам позначення.

Дужки Айверсона записуються як [*твердження*]. Вважається, що [*твердження*] = 1, якщо *твердження* істинне, та [*твердження*] = 0, якщо *твердження* хибне. Для дужок Айверсона виконується очевидна рівність $[P \wedge Q] = [P] \cdot [Q]$, де P та Q – деякі твердження.

2. Теоретичні відомості з диференціального аналізу

Нагадаємо основні означення диференціального аналізу.

Диференціал (звичайної) булевої функції f – пара двійкових векторів (α, β) така, що виконується співвідношення $f(z \oplus \alpha) \oplus f(z) = \beta$.

Імовірність диференціалу (α, β) *функції* f – величина

$$d^f(\alpha, \beta) = \frac{1}{2^q} \sum_{z \in V_q} [f(z \oplus \alpha) \oplus f(z) = \beta].$$

Вважатимемо, що диференціал є *неможливим*, якщо імовірність його існування дорівнює нулю. Якщо імовірність диференціалу дорівнює одиниці, такий диференціал назвемо *тривіальним*. Диференціали, що не є неможливими та не є тривіальними, будемо називатимемо *нетривіальними*.

Для функцій, що параметризовані ключем, диференціали розглядаються в кожній точці окремо:

Середня за ключами імовірність диференціала (α, β) *функції* f_k *в точці* z – величина

$$d^{f_k}(z, \alpha, \beta) = \frac{1}{|K|} \sum_{k \in K} [f_k(z \oplus \alpha) \oplus f_k(z) = \beta].$$

Середня імовірність диференціала (α, β) *функції* f_k – величина

$$d^{f_k}(\alpha, \beta) = \frac{1}{2^q} \sum_{z \in V_q} d^{f_k}(z, \alpha, \beta).$$

Ми також позначатимемо диференціал звичайної функції символом $\alpha \underset{f}{\to} \beta$ або просто $\alpha \to \beta$, якщо функція буде зрозуміла з контексту. Диференціал функції, що параметризована ключем, в точці z позначатимемо $\alpha \underset{f_k, z}{\to} \beta$, $\alpha \underset{f_k}{\to} \beta$, якщо з контексту зрозуміла точка, або $\alpha \to \beta$, якщо з контексту зрозуміла й функція також.

Диференціальна характеристика r-раундового ітеративного блочного шифру E – послідовність $\Omega = (\omega_0, \omega_1, ..., \omega_r) \in (V_q \setminus \{0\})^{r+1}$ така, що (ω_{i-1}, ω_i) – диференціал раундової функції $f_{k_i}^{(i)}$. Загалом диференціальною характеристикою може бути довільна послідовність ненульових двійкових векторів потрібної довжини.

Середня за ключами ймовірність диференціальної характеристики (у точці X_0) визначається як

$$DP(\Omega, X_0) = P(\omega_0 \underset{f_{k_1}^{(1)}, X_0}{\to} \omega_1, \omega_1 \underset{f_{k_2}^{(2)}, X_1}{\to} \omega_2, ..., \omega_{r-1} \underset{f_{k_r}^{(r)}, X_{r-1}}{\to} \omega_r).$$

Імовірність диференціала (ω_0, ω_r) шифру E тоді обчислюється через імовірності всіх можливих відповідних диференціальних характеристик:

$$d^E(z, \omega_0, \omega_r) = \sum_{\omega_1 \neq 0, \ldots, \omega_{r-1} \neq 0} DP(\Omega, z).$$

Перетворення називається *марковським*, якщо імовірності кожного диференціала на кожному раунді не залежать від точки входу, тобто $d^{f_k}(z, \alpha, \beta) = d^{f_k}(0, \alpha, \beta) = d^{f_k}(\alpha, \beta)$. У цьому випадку диференціальна характеристика утворює марковський ланцюг, а відповідна імовірність розбивається у добуток незалежних диференціальних імовірностей кожного раунду, що значно спрощує аналіз. Для немарковських перетворень таке розбиття буде некоректним, однак можна побудувати оцінку згори, як це показано у лемі 4.

Оцінка стійкості немарковського шифру до диференціального аналізу визначається величиною

$$MDP(E) = \max_{\alpha \neq 0, \beta, z} d^E(z, \alpha, \beta).$$

Сформулюємо декілька лем, що описують властивості диференціалів та диференціальних характеристик. Доведення цих лем можна знайти у [2, 6–11, 14–16].

Лема 1. Для довільної функції f (f_k) справедливі співвідношення:

а) $P(0 \to \beta) = [\beta = 0]$

б) $P(\alpha \to 0) = [\alpha = 0]$, якщо функція f – бієктивна (f_k – бієктивна при заданому значенні ключа).

Лема 2. Для диференціалів функції f виконуються співвідношення:

а) $\forall \alpha : \sum_{\beta} P(\alpha \underset{f}{\to} \beta) = 1.$

б) $\forall \beta : \sum_{\alpha} P(\alpha \underset{f}{\to} \beta) = 1$, якщо f – бієктивна.

Для диференціалів функції f_k, що параметризована ключем, виконуються співвідношення:

в) $\forall \alpha \forall z : \sum_{\beta} P(\alpha \underset{f_k, z}{\to} \beta) = 1.$

г) $\forall \beta \forall z : \sum_{\alpha} P(\alpha \underset{f_k, z}{\to} \beta) = 1$, якщо f_k бієктивна для кожного значення *k*.

Лема 3. Нехай q – максимальна імовірність існування нетривіального *r*-раундового диференціала ітеративного шифру. Тоді імовірність існування нетривіального $(r+1)$-раундового диференціала того самого шифру не перевищує q.

Лема 4. Для *r*-раундової диференціальної характеристики $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ ітеративного шифру E_K виконується нерівність:

$$\forall z : DP(\Omega, z) \leq \prod_{i=1}^{r} \max_x d^{f_{k_i}^{(i)}}(x, \omega_{i-1}, \omega_i).$$

3. Основні результати

Аналітичні оцінки верхньої межі імовірності існування нетривіальних диференціалів немарковських схеми Фейстеля та MISTY-схеми були вперше одержані Ковальчук у [15]. Наведемо ці результати у вигляді наступних двох теорем.

Теорема 1 *(Ковальчук)*

Нехай $E = \Psi[f_1, f_2, f_3]$ – трираундова схема Фейстеля, раундові функції якої бієктивні за кожного значення ключа, а $p = \max\{MDP(f_1), MDP(f_2), MDP(f_3)\}$. Тоді існує співвідношення:

$$MDP(E) \le p^2,$$

тобто імовірність довільного нетривіального трираундового диференціала E не перевищує величини p^2.

Теорема 2 *(Ковальчук)*

Нехай $E = L[f_1, f_2, f_3]$ – трираундова L-схема, раундові функції якої бієктивні за кожного значення ключа, а $p = \max\{MDP(f_1), MDP(f_2), MDP(f_3)\}$. Тоді існує співвідношення:

$$MDP(E) \le p^2,$$

тобто імовірність довільного нетривіального трираундового диференціала E не перевищує величини p^2.

Зауважимо, що ці результати аналогічні оцінкам, які було одержано для марковських DES-подібних шифрів: Аокі та Отою для схеми Фейстеля, Мацуі для L-схеми, Канеко, Сано та Сакураі для R-схеми. У наступній теоремі ми подамо аналогічні, але уточнені оцінки для диференціальних імовірностей *R*-схеми.

Теорема 3

Нехай $E = R[f_1, f_2, f_3]$ – трираундова *R*-схема, раундові функції якої бієктивні за кожного значення ключа, і $p_i = MDP(f_i)$, $i = \overline{1,3}$. Тоді існує співвідношення:

$$MDP(E) \le \max\{p_1 p_2,\ p_1 p_3,\ p_2 p_3\}.$$

Доведення. Зафіксуємо деяку вхідну точку $X = (x_1, x_2)$ та розглянемо довільну нетривіальну диференціальну характеристику $\Omega = (\omega_0, \omega_1, \omega_2, \omega_3)$ (для зручності запису ми будемо опускати відповідні вхідні точки). Зі схеми шифрування видно, що якщо $P(\Omega) \ne 0$, то мають виконуватись такі співвідношення: $\omega_0 = (a_1, a_2)$, $\omega_1 = (a_2 \oplus b_1, b_1)$, $\omega_2 = (c_2 \oplus b_1, c_2)$, $\omega_3 = (c_1, c_2)$, де a_1, a_2, b_1, c_1, c_2 – деякі бітові вектори. Отже,

$$DP(\Omega, X) = P\left(a_1 \underset{(1)}{\to} b_1,\ a_2 \oplus b_1 \underset{(2)}{\to} c_2,\ c_2 \oplus b_1 \underset{(3)}{\to} c_1 \right)$$

(тут число у дужках під стрілочками показує номер раундової функції).

Для довільного нетривіального диференціала (a, c) маємо:

$$d^E(X, a, c) = \sum_{b_1} DP(\Omega, X), \text{ де } \omega_0 = a,\ \omega_3 = c,$$

тобто, при фіксуванні вхідної та вихідної різниць в характеристиці залишається невизначеною лише змінна b_1.

Очевидно, що за різних значень (a, c) деякі з диференціальних переходів тривіалізуються. Розглянемо всі можливі випадки.

1. Нехай $a_1 = 0$. За лемою 1 маємо $a_2 \ne 0$ та $b_1 = 0$. Значення b_1 фіксується, тому

$$d^E(X, a, c) = P\left(a_2 \underset{(2)}{\to} c_2,\ c_2 \underset{(3)}{\to} c_1 \right) \le p_2 p_3.$$

2. Нехай тепер $a_1 \ne 0$, але $c_1 = 0$; тоді $c_2 \ne 0$ та $b_1 = c_2 \ne 0$ (також за лемою 1). Значення b_1 знов фіксується, отже, маємо:

$$d^E(X, a, c) = P\left(a_1 \underset{(1)}{\to} c_2,\ a_2 \oplus c_2 \underset{(2)}{\to} c_2 \right) \le p_1 p_2.$$

3. Нехай тепер $a_1 \neq 0$, $c_1 \neq 0$, але $c_2 = 0$. У цьому випадку $b_1 = a_2$ та $b_1 \neq 0$, а тому

$$d^E(X,a,c) = P\left(a_1 \underset{(1)}{\to} a_2,\ c_2 \underset{(3)}{\to} c_1 \right) \leq p_1 p_3 .$$

4. Нарешті, нехай $a_1 \neq 0$, $c_1 \neq 0$ та $c_2 \neq 0$. У цьому випадку значення b_1 не фіксується, отже, можемо записати:

$$d^E(X,a,c) = \sum_{b_1} P\left(a_1 \underset{(1)}{\to} b_1,\ a_2 \oplus b_1 \underset{(2)}{\to} c_2,\ c_2 \oplus b_1 \underset{(3)}{\to} c_1 \right) =$$

$$= \sum_{b_1} P\left(a_1 \underset{(1)}{\to} b_1 \right) \cdot P\left(a_2 \oplus b_1 \underset{(2)}{\to} c_2,\ c_2 \oplus b_1 \underset{(3)}{\to} c_1 \mid b_1 \right) \leq p_2 p_3 \sum_{b_1} P\left(a_1 \underset{(1)}{\to} b_1 \right) = p_2 p_3 ,$$

де ми спочатку застосували лему 4, а потім – лему 2.

Підсумовуючи всі випадки, бачимо, що $d^E(X,a,c) \leq \max\{p_1 p_2,\ p_1 p_3,\ p_2 p_3\}$ для довільного диференціала (a,c) та довільної точки *X*, звідки й випливає твердження теореми.

Наслідок. Якщо $p = \max\{p_1,\ p_2,\ p_3\}$, то $MDP(E) \leq p^2$.

Отже, ми можемо знайти верхню межу імовірності існування нетривіальних трираундових диференціалів R-схеми, використовуючи відповідні параметри раундових функцій. Оскільки раундові функції R-схеми мають вдвічі меншу розмірність, знайти їх диференціальні імовірності значно легше в обчислювальному плані.

З леми 3 випливає, що одержана оцінка буде справедливою для довільного *r*-раундового диференціала R-схеми при $r \geq 3$. Отже, за теоремою 3 можна встановити доказову (теоретичну) стійкість шифрів, побудованих на основі R-схеми, до диференціального аналізу.

З теореми 3 також безпосередньо можна одержати оцінки практичної стійкості – оцінки верхньої межі імовірності існування довільних диференціальних характеристик. Цю оцінку подамо у теоремі 4.

Теорема 4. Нехай $E = R[f_1, f_2, ..., f_r]$ – *r*-раундова *R*-схема, раундові функції якої бієктивні за кожного значення ключа, і $p = \max\limits_i MDP(f_i)$. Тоді для довільної диференціальної характеристики Ω та довільної вхідної точки *X* існує співвідношення:

$$DP(\Omega, X) \leq p^{2\left\lfloor \frac{r}{3} \right\rfloor}.$$

Доведення. З доведення теореми 3 випливає, що з довільних послідовних трьох раундів *R*-схеми тривіалізуватись може не більше одного, тобто з трьох послідовних раундів щонайменше два будуть нетривіальними. Звідси одразу ж випливає твердження теореми 4.

Потрібно зауважити, що для схеми Фейстеля та L-схеми існують аналогічні уточнені оцінки як для імовірностей диференціалів, так і для імовірностей диференціальних характеристик. Доведення цих фактів майже ідентичне доведенню теорем 3 та 4.

Висновки

У цій роботі ми навели аналітичні оцінки верхніх меж імовірностей існування нетривіальних диференціалів та диференціальних характеристик для R-схеми блочного шифрування у загальному вигляді. Такі оцінки є параметрами, що визначають доказову (теоретичну) та практичну стійкість блочних шифрів, побудованих на основі R-схеми, до диференціального криптоаналізу. Зауважимо, що, на відміну від попередньо опублікованих результатів, одержані нами оцінки є точніші та справедливі для загального випадку немарковських шифрів.

Результати цієї роботи можна застосовувати для теоретичного та практичного оцінювання стійкості до диференціального криптоаналізу як складніших схем блочного шифрування, так і конкретних алгоритмів.

1. Feistel H. Cryptography and Computer Privacy – Scientific American, v. 228, n. 5, May 1973, pp. 15–23. 2. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis – IEICE Trans. Fundamentals, vol. E82-A – 1999 – #1 – P. 117–122. 3. Gilbert H., Minier M. New Results on the Pseudorandomness of Some Blockcipher Constructions – Lecture Notes in Computer Science, 2002, Volume 2355, Fast Software Encryption. – P. 159–178 4. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3–72. 5. Biham E., Shamir A. Differential cryptanalysis of the full 16-round DES // Advances in Cryptology – CRYPTO'92, Proceedings. – Springer Verlag, 1993. – P. 487–496. 6. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17–38. 7. O'Connor L., Golic J.D. A unified Markov approach to differential and linear cryptanalysis // Advances in Cryptology – ASIACRYPT'94, Proceedings. – Springer Verlag, 1994. – P. 387–397. 8. Nyberg K., Knudsen L.R. Provable Security Against a Differential Attack // Journal of Cryptology, Vol. 8, no. 1 (1995). 9. Aoki K., Ohta K. Stricter Evaluation for the Maximum Average of Differential Probability and the Maximum Average of Linear Probability // Proceedings of SCIS'96, SCIS96-4A (1996) (японською мовою). 10. Kaneko Y., Sano F. and Sakurai K. On Provable Security against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Multiple Random Functions – Proc. of SAC'97, 1997, pp. 185–199. 11. Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260–274. 12. Knudsen L.R. Practically secure Feistel cipher // Fast Software Encryption. – FSE'94, Proceedings. – Springer Verlag, 1994. – P. 211–221. 13. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. – SAC 2000, Proceedings. – Springer Verlag, 2001. – P. 324–338. 14. Ковальчук Л.В. Обобщенные марковские шифры: построение оценки практической стойкости относительно дифференциального криптоанализа // Математика и безопасность информационных технологий. Материалы конференции в МГУ 25–27 октября 2006 г. – М.: МЦНМО, 2007. – С. 595–599. 15. Ковальчук Л.В., Шерстюк А.О. Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2 // Прикладная радиоэлектроника. – 2009. – № 3. – С. 15–27. 16. Ковальчук Л.В., Пальченко С.В., Скрипник Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – К.: НДЦ «Тезіс», 2009. – № 2 (19). – С. 45–56.