УДК 681.3.06:006.354

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКОВАНИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ УКРАЇНИ ТА РОСІЇ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Л. В. КОВАЛЬЧУК, Н. В. КУЧИНСЬКА

Розглянуто одну з актуальних модифікацій різницевого криптоаналізу, а саме цілочисельний різницевий криптоаналіз. Отримано науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу модифікованих стандартів блокового шифрування України та Росії. Показано від яких саме параметрів, що характеризують s-блоки, залежать ці оцінки. Проведено порівняльний аналіз значень цих параметрів для всіх алгоритмів, розглянутих у цій роботі. Також наведено статистичний розподіл отриманих параметрів за випадковою вибіркою з 100000 s-блоків.

Ключові слова: різницевий криптоаналіз, стандарти блокового шифрування, s-блоки.

ВСТУП

Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності під час обробки інформації в сучасних інформаційно-телекомунікаційних системах. Тривалий час у країнах СНД широко використовувався радянський алгоритм блокового шифрування ГОСТ 28147-89. Але питання його удосконалення та побудови нових ефективних алгоритмів шифрування з обґрунтованою стійкістю залишилось актуальним. В результаті за останні кілька років в країнах СНД було прийнято низку власних стандартів блокових шифрів:

- СТБ 34.101.31-2011 (Білорусь) [1];
- ГОСТ Р 34.12 2015 (РФ) [2];
- ДСТУ 7624:2014 «Калина» (Україна) [3].

Слід зауважити, що в стандарті ГОСТ Р 34.12 2015 визначено два алгоритми блокового шифрування: один алгоритм для довжини блока 128 біт, на який можна посилатись, як на «Кузнєчік», другий алгоритм з довжиною блока 64 біт, на який можна посилатись, як на «Магму». Другий алгоритм є за своєю структурою аналогічним алгоритму, визначеному в ГОСТ 28147-89 [2]. Крім того, український («Калина») та російський («Кузнєчік») стандарти схожі за своєю будовою, оскільки за основу обох алгоритмів було взято стандарт AES. У цьому розумінні алгоритм ГОСТ Р 34.12 2015 «Кузнєчік» можна вважати «Калина»–подібним алгоритмом.

Переважну більшість сучасних блокових SPN-шифрів спроектовано схожим чином: їх раундові функції є композицією ключового суматора, блоку підстановки і оператора перестановки, лінійного над полем F_2 або його деяким розширенням. Тому задача оцінювання стійкості таких шифрів до різницевого криптоаналізу та його можливих модифікацій або зводиться до задачі побудови верхніх оцінок середніх ймовірностей диференціалів таких композицій, або містить її як підзадачу [4–15].

Вперше цілочисельні диференціали згадуються у роботах, що стосуються криптоаналізу та обґрунтування стійкості геш-функцій. Зокрема, з використанням цілочисельних диференціалів були побудовані колізії як до багатьох функцій класу MD, так і до окремих вузлів таких функцій. Досить повний перелік посилань на такі роботи, а також обґрунтування використання саме цілочисельних диференціалів можна знайти в [8–10]. Зауважимо, що аналітичні складнощі, які виникають в цьому випадку у зв'язку з наявністю біта переносу при модульному додаванні, посилюються тим, що оператор перестановки, який є одним з перетворень хеш-функції, не є лінійним відносно модульного додавання. Виходячи з отриманих у роботах [8–10] результатів, можна зробити висновок, що використання цілочисельних диференціалів є виправданим при криптоаналізі таких блокових шифрів або хеш-функцій, які містять суматор за модулем 2^n, причому як правило n=32 або 64.

Слід зазначити, що у всіх попередніх роботах, у яких розглядались немарковські та узагальнено марковські блокові шифри, або будувались оцінки практичної стійкості алгоритмів відносно побітового різницевого криптоаналізу, або будувались оцінки стійкості раундових функцій до цілочисельного криптоаналізу. Питання побудови оцінок стійкості блокових алгоритмів до цілочисельного різницевого криптоаналізу у цій роботі розглянуто вперше.

Основні означення, що стосуються марковських, узагальнено марковських блокових алгоритмів та такі, що використовуватимемо в даній статті, можна знайти в [5, 13].

1. ОСНОВНІ ТЕРМІНИ ТА ПОЗНАЧЕННЯ

Розглянемо $\Im$ – r-раундовий блоковий шифр, який перетворює відкритий текст $x \in V_n$ у шифрований текст $y \in V_n$ при ключі шифрування $k = (k_1, k_2, \ldots, k_r) \in (V_m)^r$ за таким правилом:

$$y = \Im_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \cdots \circ f_{k_1}(x), \qquad (1)$$

де $k_i \in V_m$, $i = \overline{1, r}$ – раундові ключі, $f_\lambda(\cdot) : V_n \to V_n$, $\lambda \in V_m$ – раундова функція шифрування. Також припускатимемо, що раундові ключі незалежні в сукупності рівноімовірно розподілені на V_m випадкові величини.

Для раундової функції $f_k : V_n \to V_n, k \in V_m$, яка фігурує в (1), *диференціалом (різницею) цієї функції відносно операцій* (μ_1, μ_2) називатимемо пару (α, β), для яких існує $x \in V_n$ таке, що виконується співвідношення:

$$f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1} = \beta,$$

де $\alpha, \beta \in V_n$, а під $f_k(x)^{-1}$ розуміють елемент множини V_n, обернений до $f_k(x)$ відносно операції μ_2 [13]. У такому випадку двійковий вектор α називають вхідною різницею, а β - вихідною.

Величину

$$d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1}, \beta), \quad (2)$$

називають *середньою* (*за ключами*) *ймовірністю раундового диференціалу* (α, β) *в точці* x відносно операцій μ_1, μ_2 на множині V_n, де $x, \alpha, \beta \in V_n$.

Величину

$$d^f_{\mu_1,\mu_2}(\alpha, \beta) = 2^{-n} \sum_{x \in V_n} d^f_{\mu_1,\mu_2}(x; \alpha, \beta) \quad (3)$$

називають *середньою* (*за ключами*) *ймовірністю раундового диференціалу* (α, β) відносно операцій μ_1, μ_2 [13]. Якщо $\mu_1 = \mu_2 = \mu$, також використовуватимемо позначення $d^f_\mu(x; \alpha, \beta)$ і $d^f_\mu(\alpha, \beta)$, якщо це не викликає непорозумінь.

За означенням, шифр є марковським, якщо $\forall\ x, \alpha, \beta \in V_n$: $d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(0; \alpha, \beta)$.

З (3) випливає, що в цьому випадку також правильно

$$\forall\ x, \alpha, \beta \in V_n : d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(\alpha, \beta).$$

Різницевою характеристикою шифру (1) назвемо послідовність $\Omega = (\omega_0, \omega_1, \ldots, \omega_{r+1})$, де $\omega_i \in V_n \setminus \{0\}$, $i = \overline{1, r}$. [5]

Середньою (за ключами) ймовірністю різницевої характеристики назвемо величину

$$EDP(\Omega) =$$

$$= \frac{1}{2^n} \sum_{x_0 \in V_m} \frac{1}{2^{mr}} \sum_{k_1, \ldots, k_r \in V_n} \prod_{i=1}^{r} \delta(f_{k_i}(x_{i-1} \circ \omega_{i-1}) \circ f_{k_1}^{-1}(x_{i-1}), \omega_i) \cdot$$

Ми розглядатимемо лише такі Ω, для яких $EDP(\Omega) \neq 0$. Зауважимо, що введена таким чином величина $EDP(\Omega)$ дійсно є імовірністю (за всіма $K \in (V_m)^r$ та $x_0 \in V_n$) події, яка полягає у тому, що вхідна різниця ω_0 після першого раунду перейшла у різницю ω_1, після другого – у ω_2 і т. д., а після r-го – у ω_r. Величина $\max_\Omega EDP(\Omega)$ є обернено пропорційною до кількості матеріалу, необхідного для атаки на алгоритм, тобто вона характеризує *практичну стійкість блокового алгоритму шифрування*.

Оскільки дослідження стійкості марковських та немарковських блокових шифрів суттєво відрізняється, то в ході аналізу будь-якого блокового шифру на першому етапі завжди потрібно визначити, чи є він марковським.

У наших позначеннях марковський шифр має такі властивості:

1) величина (2) не залежить від x і дорівнює середній (за ключами) імовірності раундового диференціалу у точці 0;

2) для величини (3) виконується така рівність:
$\forall \alpha, \beta \in V_m\ \forall x \in V_m$:

$$d^f_{\mu_1,\mu_2}(\alpha, \beta) = d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(0; \alpha, \beta),$$

тобто середня за ключами імовірність раундового диференціалу дорівнює середній за ключами імовірності раундового диференціалу у точці 0.

Основною властивістю марковських шифрів, яка водночас є їхньою суттєвою перевагою в ході побудови оцінок практичної стійкості до різницевого криптоаналізу, є виконання такого співвідношення:

$$EDP(\Omega) = \prod_{i=0}^{r-1} d^f_{\mu_1,\mu_2}(0; \omega_i, \omega_{i+1}) = \prod_{i=0}^{r-1} d^f_{\mu_1,\mu_2}(\omega_i, \omega_{i+1}),$$

тобто імовірність різницевої характеристики марковського шифру дорівнює добутку імовірностей його раундових диференціалів у точці 0.

2. ПОБУДОВА ОЦІНОК ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКОВАНОГО ГОСТ-ПОДІБНОГО АЛГОРИТМУ

Означення 1. Називатимемо блоковий алгоритм шифрування (1) *модифікованим ГОСТ-подібним алгоритмом*, якщо його раундова функція має такий вигляд:

$$f_k(u, v) = (v, u + \varphi(v + k)), \quad (4)$$

де $x = (u, v) \in V_n$, $n = 2m$, $u, v, k \in V_m$, k – раундовий ключ, $\varphi : V_m \times V_m \to V_m$ – раундове перетворення алгоритму (4), а під операцією "+" розуміють додавання за модулем 2^m.

Довжина блоку алгоритму визначається як $n = pu$, $p \geq 2$, а блок підстановки є відображенням, визначеним таким чином:

$$\forall x \in V_n : \quad S(x) = (s^{(p)}(x^{(p)}), \ldots, s^{(1)}(x^{(1)})),$$

$$x^{(i)} \in V_u, i = \overline{1, p},$$

де s-блоки $s^{(i)}: V_u \to V_u$, $i = \overline{1, p}$ – бієктивні відображення.

Відображення зсуву вліво на t біт вектора з V_m позначимо $L_t: V_m \to V_m$.

В наших позначеннях раундове перетворення $\varphi: V_m \times V_m \to V_m$, яке задано в (4), можна подати таким чином:

$$\varphi(x,k) = L_t\big(S(x+k)\big). \qquad (5)$$

Для модифікованого за таким правилом алгоритму справедливі наступні леми.

Лема 1. Блоковий алгоритм шифрування з раундовою функцією (4) є марковським шифром відносно операції додавання за модулем 2^m.

Доведення леми 1 виконується заміною змінної $k+v$ на k під час обчислення (2).

Лема 2. Для модифікованого ГОСТ-подібного алгоритму справедлива така оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max_{\alpha,\beta \in V_n \setminus \{0\}} d_+^{\varphi}(0;\alpha,\beta) \right)^{\left\lfloor \frac{2r}{3} \right\rfloor}.$$

Доведення леми 2 є аналогічним до доведення відповідного результату у роботі [9] для класичного різницевого криптоаналізу.

Для побудови верхньої оцінки величини $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d_+^{\varphi}(0;\alpha,\beta)$ скористаємось результатами, отриманими в [15, 16]. Далі ми коротко наведемо ці результати.

Введемо необхідні позначення.

Для довільного блоку заміни s покладемо

$$\Delta_+^s = \max_{\alpha,\beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(s(k+\alpha) - s(k), \beta), \quad (6)$$

$$\delta_+^s = \max_{\substack{\alpha \in V_u \setminus \{0\} \\ \beta \in V_u \setminus \{0\}}} \frac{1}{2^u} \sum_{k \in V_u} (\delta(s(k+\alpha) - s(k), \beta) +$$

$$+ \delta(s(k+\alpha) - s(k), \beta + 1)). \qquad (7)$$

Таким чином верхні оцінки середніх імовірностей цілочисельних диференціалів відображення (5) визначає наступна теорема [15].

Теорема 1. Нехай $t \ge u, p \ge 2$. Якщо раундова функція має вигляд (5), то справедлива така нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\}: \quad d_+^{\varphi}(\alpha,\beta) \le \max\left\{ \delta_+^s,\ 2\Delta_+ \right\}.$$

Тому шукане найбільше значення γ відповідно буде

$$d_+^{\varphi}(\alpha,\beta) \le \gamma = \max\left\{ \delta_+^s,\ 2\Delta_+ \right\}. \qquad (8)$$

Зауважимо, що час обчислення параметра (8) для довжини входу $n = pu$ (розмір входу s-блоку дорівнює u) становить $O(pu^3 \log u)$ бітових операцій.

Використовуючи результати лем 1, 2 та теореми 1 можна довести справедливість оцінки практичної стійкості модифікованого ГОСТ-подібного алгоритму до цілочисельного різницевого криптоаналізу. Для введеного ГОСТ-подібного алгоритму справедливим є наступний результат.

Теорема 2. Для модифікованого ГОСТ-подібного алгоритму справедлива оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max\left\{ \delta_+^s,\ 2\Delta_+ \right\} \right)^{21}.$$

Нижче наведено статистичний розподіл параметрів (6), (7) для вузлів заміни алгоритму ГОСТ, рекомендованих згідно з [17].

Таблиця 1

Значення параметрів (6), (7) для рекомендованих вузлів заміни алгоритму ГОСТ

Номер ДКЕ	*вузол заміни*	*значення вузла заміни*	$2^4 \cdot d_+^s$	$2^4\ \delta_+^s$
dke1	K0	a9d6eb45f13c7082	4	7
dke1	K1	80c4967b231f5ead	4	5
dke1	K2	f658eba4c037291d	5	6
dke1	K3	38d96bf025ca4e17	4	7
dke1	K4	f8e9720dc615b43a	4	6
dke1	K5	28975f0bc1dea364	5	7
dke1	K6	38b564ea2c179fd0	5	5
dke1	K7	123e6db8fac57904	5	6
dke2	K0	e937f4cb6ad10582	4	7
dke2	K1	adc76e81f3b40952	4	6
dke2	K2	4b1f92ec6a87350d	4	6
dke2	K3	451c7e92afbd0863	4	5
dke2	K4	cb39f04572ed1a86	4	5
dke2	K5	873a96e5d04c12fb	4	6
dke2	K6	f0e68d59a31c4b72	3	5
dke2	K7	43ed502b1a769f8c	4	6
dke3	K0	d91e72c54b6f38a0	5	7
dke3	K1	786b034d95feac21	3	5
dke3	K2	a53c98d64fe02b17	5	5
dke3	K3	bac1569e2df70438	4	6
dke3	K4	5b30f9e41c862a7d	4	5
dke3	K5	43bd1f827ec9a065	3	5
dke3	K6	378b1e50d4ca29f6	5	6
dke3	K7	6dcab793fe120845	4	5
dke4	K0	9c3d76e1a2048f5b	3	5
dke4	K1	a5be760c28f4d391	5	6
dke4	K2	4c30d2eb7f5918a6	5	6
dke4	K3	3945e786d02fbca1	5	7
dke4	K4	29cfdb41753e68a0	4	6
dke4	K5	e5db1942f8703ca6	4	7
dke4	K6	e65a9d48bc0371f2	4	7
dke4	K7	19cb76832fe05a4d	4	7

Номер ДКЕ	*вузол заміни*	*значення вузла заміни*	$2^4 \cdot d_+^s$	$2^4\ \delta_+^s$
dke5	K0	34d8c7a20e9fb156	3	5
dke5	K1	c76938b5fa0d421e	5	5
dke5	K2	e487b3ac1269df05	5	6
dke5	K3	396d8fa27ec0b415	6	8
dke5	K4	5ca721fde3b40896	4	6
dke5	K5	18be74a0c35d9f62	6	7
dke5	K6	9bad5e23064cf178	4	5
dke5	K7	e9185fb062c7a4d3	4	6
dke6	K0	fc96e21b0d4a7835	5	6
dke6	K1	ec5074a3261d9bf8	3	6
dke6	K2	56d9bea3f281407c	4	6
dke6	K3	1f742ec36b9805ad	4	6
dke6	K4	f9e6d158423cab07	6	6
dke6	K5	b0d7ce142368a5f9	5	7
dke6	K6	7ef8d0b3a1429c65	4	6
dke6	K7	15eb2c38a097f64d	5	8
dke7	K0	fda5c01692e73b48	5	6
dke7	K1	25a0691fd47eb38c	4	6
dke7	K2	3e4b5912f68d70ac	6	6
dke7	K3	4ab9f2e5d13607c8	4	6
dke7	K4	f65897cb0a3124de	4	6
dke7	K5	cbf451e908d2a736	4	6
dke7	K6	d248bc13a59e7f06	4	6
dke7	K7	150f6a3e72cdb894	4	5
dke8	K0	e4b2875c9d031f6a	5	7
dke8	K1	3eca62d198740f5b	5	6
dke8	K2	52871fe64db0a3c9	4	5
dke8	K3	ca7de3029516b4f8	4	7
dke8	K4	63f709a8bc4152de	4	6
dke8	K5	6df15380bae49c27	4	5
dke8	K6	2fc5b13e06da7948	4	6
dke8	K7	305c8fdeb629714a	5	6
dke9	K0	90bc243fd6e1a758	4	6
dke9	K1	350f87ecda16b249	5	6
dke9	K2	845aebd6cf793120	4	6
dke9	K3	54f0cba91e8632d7	5	7
dke9	K4	7c3068eb1fda9524	4	6
dke9	K5	743b6a819ced0f25	4	6
dke9	K6	7e9f1483bd026a5c	4	6
dke9	K7	e28f307cbd15649a	5	7
dke10	K0	8469bc1237e0daf5	4	6
dke10	K1	7d18ae4f90632cb5	4	6
dke10	K2	c8d1a29634e75f0b	3	5
dke10	K3	2b34c79df8501ea6	4	6
dke10	K4	83daef5147bc2069	6	7
dke10	K5	4c9bea76350f128d	5	6
dke10	K6	58e7301da692fbc4	7	7
dke10	K7	a3590d78c416bf2e	5	9

Нижче наведено статистичний розподіл параметрів для чотирьох та восьми бітових вузлів заміни, згенерованих випадково та рівноймовірно.

Аналізуючи результати статистичного дослідження розподілу параметрів для чотирьохбітових та восьмибітових s-блоків, зокрема, було знайдено підстановки з найменшими можливими значеннями параметрів (6) та (7), використання яких дозволить підвищити стійкість раундових перетворень по відношенню до цілочисельного різницевого криптоаналізу. Виходячи з отриманих результатів, верхні оцінки імовірностей цілочисельного раундового диференціалу для відображення (5) при відповідному виборі s-блоків можуть приймати значення $d_+^{\varphi}(\alpha,\beta) \le 0{,}04$.

Таблиця 2

Зведені значення параметрів (6)–(7) для вузлів заміни алгоритму ГОСТ

Значення δ_+^s	Кількість вузлів заміни	Значення Δ_+	Кількість вузлів заміни
0,1875	7	0,3125	18
0,25	43	0,375	42
0,3125	24	0,4375	17
0,375	5	0,5	2
0,4375	1	0,5625	1

Таблиця 3

Статистичний розподіл параметрів (6)–(7) для чотирьохбітових вузлів заміни (вибірка з 10000 підстановок)

Значення $d_+^{s(j)}$	Кількість підстановок	Значення $\delta_+^{s(j)}$	Кількість підстановок
0,1875	816	0,25	39
0,25	5305	0,3125	2254
0,3125	2920	0,375	4578
0,375	790	0,4375	2302
0,4375	131	0,5	668
0,375	37	0,5625	134
0,4375	1	0,625	20
		0,6875	5

Таблиця 4

Статистичний розподіл параметрів (6)–(7) восьмибітових вузлів заміни (вибірка з 10000 підстановок)

Значення $d_+^{s(j)}$	Кількість підстановок	Значення $\delta_+^{s(j)}$	Кількість підстановок
0.0195315	13	0,03125	8
0.0234375	4744	0,03515625	2520
0.0273438	4458	0,0390625	5235
0.03125	724	0,04296875	1836
0.0351563	57	0,046875	340
0.0390625	3	0,05078125	54
0.0429688	1	0,0546875	7

У такому випадку, якщо чотирибітові вузли заміни обрані з рекомендованих [17], але з найменшими значеннями параметрів (dke2 або dke7) такими, що $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i, \omega_{i+1}) \le 2 \cdot 0{,}375$, тоді може бути отримана оцінка виду $\max\limits_{\Omega} EDP(\Omega) \le 0{,}0024 \approx 2^{-9}$.

Звичайно, ця оцінка стійкості є надзвичайно

низькою. Але вона суттєво покращиться, якщо обрати чотирибітові вузли заміни так щоб $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2\cdot 0{,}1875$. Тоді буде справедливою оцінка $\max\limits_{\Omega} EDP(\Omega) \le 1{,}13\cdot 10^{-9} \approx 2^{-29}$.

Нижче наведено приклади s-блоків (представлені у різному вигляді), які мають найменше значення відповідного параметра (8):

1)	11 15 14 7 8 12 3 1 13 10 4 5 0 9 6 2	bfe78c31da450962
2)	2 13 11 7 10 1 9 12 5 3 14 4 0 6 15 8	2db7a19c53e406f8
3)	7 0 9 2 3 11 1 13 10 8 5 4 6 14 15 12	70923b1da8546efc
4)	15 7 9 2 0 12 4 6 10 11 3 13 8 5 14 1	f7920c46ab3d85e1

Якщо ж у модифіканому алгоритмі ГОСТ використовувати 8-бітових вузлів заміни і обрати їх так, щоб $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2\cdot 0{,}0195,$ то $\max\limits_{\Omega} EDP(\Omega) \le 2{,}58\cdot 10^{-30} \approx 2^{-98}$, що є дуже гарною оцінкою для алгоритму з 64-бітовим блоком.

Нижче наведено приклади s-блоків, які мають найменше значення відповідного параметра (8):

150 162 116 70 253 232 248 182 24 32 106 27 240 84 138 203 62 202 155 213 40 176 114 143 151 113 228 217 88 178 140 8 223 205 225 243 141 14 55 210 112 128 255 42 110 9 144 72 187 177 197 237 86 87 28 224 100 115 11 7 53 75 132 241 66 164 49 41 77 5 59 130 199 63 179 50 221 149 21 35 65 124 126 137 191 67 93 198 222 148 215 61 163 82 108 171 250 211 229 6 73 239 109 233 201 90 244 71 218 10 242 168 254 204 251 165 74 235 107 159 120 188 104 105 167 136 44 207 180 194 20 216 2 238 152 60 154 31 46 0 47 166 122 36 175 54 234 125 34 135 80 226 153 169 15 26 193 101 146 127 68 1 64 56 156 118 48 246 57 103 209 89 134 196 3 247 123 4 157 102 38 81 99 186 173 18 161 129 119 208 58 17 236 22 227 98 96 190 13 43 195 172 139 214 192 212 189 51 94 25 19 37 29 117 16 76 174 79 230 33 131 245 231 91 145 23 206 95 249 147 78 97 111 158 121 185 69 133 184 219 160 85 183 30 92 170 252 181 142 220 45 200 83 52 39 12

251 84 128 186 236 221 168 132 198 115 119 210 143 66 110 73 19 96 27 38 30 140 196 92 120 56 60 1 62 237 239 46 26 75 188 32 226 136 72 156 145 78 70 170 36 202 21 241 243 55 109 6 0 4 209 50 183 116 101 105 51 125 144 67 181 11 222 53 74 164 134 79 98 249 227 147 107 108 180 28 246 200 154 152 174 254 102 248 161 214 160 117 151 225 139 69 166 148 121 190 250 178 171 9 61 252 135 233 234 142 94 16 89 218 34 219 217 12 64 155 68 29 58 187 17 127 216 157 167 82 182 54 13 201 76 95 137 106 113 203 103 71 123 81 146 104 215 90 229 42 194 93 83 191 5 195 213 208 176 138 245 10 207 173 8 158 230 87 2 255 228 63 99 244 52 165 131 126 24 3 118 206 57 232 184 39 77 122 35 197 15 48 43 129 111 59 45 44 220 235 49 179 40 85 224 189 65 20 162 130 149 7 37 153 112 25 150 100 169 242 240 177 41 247 31 47 86 212 141 253 114 33 159 193 231 124 91 238 192 204 14 223 163 211 22 172 205 80 23 185 175 18 199 97 88 133

21 192 199 134 128 248 112 175 1 144 85 203 181 163 73 189 170 67 206 60 174 253 178 51 46 99 240 61 148 244 146 149 2 162 9 43 98 235 38 165 105 116 81 160 236 230 86 138 216 197 62 114 23 218 19 252 221 157 182 79 54 122 93 65 49 229 215 92 75 202 129 242 187 241 22 123 72 191 117 223 176 195 151 226 237 7 219 198 90 124 246 100 8 196 210 97 193 17 211 168 50 250 30 78 205 222 80 183 121 69 156 251 245 201 66 131 239 24 34 16 106 180 76 83 190 130 108 44 255 249 152 10 126 166 217 47 140 228 159 161 53 188 139 143 167 109 213 59 40 234 102 15 145 186 45 74 142 150 71 172 232 89 70 14 94 169 84 207 185 25 11 173 200 31 135 209 57 0 154 26 18 184 27 39 254 243 208 119 6 153 104 194 179 3 158 48 35 64 58 136 225 55 68 141 37 212 87 125 238 63 77 29 137 5 231 204 214 247 113 227 91 88 33 20 13 133 110 32 171 127 147 103 120 4 155 107 28 96 82 233 132 41 12 101 224 115 164 42 95 177 56 52 36 118 111 220

48 149 75 141 241 252 180 153 128 184 247 62 136 54 181 129 82 56 131 33 161 101 107 63 5 251 227 183 171 37 90 239 228 250 218 150 59 23 12 179 2 145 115 219 203 211 49 106 111 126 213 0 215 249 159 209 204 123 60 135 89 142 199 8 73 221 160 248 164 80 91 88 173 214 143 98 86 127 232 156 19 166 193 139 185 122 114 109 169 95 216 104 125 176 225 24 220 240 100 110 175 144 27 116 163 217 229 105 255 22 40 78 174 92 197 50 200 157 238 113 67 20 34 36 76 120 177 230 25 162 93 108 134 47 190 9 235 158 155 178 26 189 70 28 130 87 226 31 187 233 245 236 196 16 55 1 79 42 77 97 212 152 52 186 46 254 231 210 118 119 138 165 207 14 253 223 44 112 84 65 10 151 198 45 71 53 148 172 246 99 4 117 17 132 66 237 121 29 182 43 195 15 96 83 85 102 146 3 201 194 7 30 147 57 222 137 206 64 188 124 13 39 234 41 224 72 32 69 58 191

103 18 74 244 61 242 94 140 21 51 81 11 68
133 202 208 6 35 167 168 205 154 192 170 38
243

145 38 250 181 173 130 111 157 95 97
198 47 210 238 131 120 221 77 124 90 3 193
217 12 154 234 23 236 64 192 21 36 24 244
107 172 72 13 70 79 218 117 220 61 179 92
253 51 49 116 200 165 87 101 18 186 170 249
54 137 33 209 205 134 140 41 188 46 7 65
232 5 161 183 223 91 103 60 224 214 6 88
168 123 81 99 164 229 248 82 68 151 167 149
171 146 102 85 55 121 28 74 128 251 246 174
129 86 178 166 194 255 30 132 4 62 201 254
20 66 212 94 184 22 240 189 1 233 10 242
182 98 135 96 235 32 219 8 163 144 222 204
17 80 191 206 228 225 215 158 76 50 147 19
125 208 160 143 190 48 185 73 37 42 45 115
58 177 100 63 11 227 226 136 199 247 187 84
35 40 197 142 207 75 29 83 239 105 69 153
106 109 31 119 169 27 216 211 122 133 110 114
175 152 11

3. ПОБУДОВА ОЦІНОК ПРАКТИЧНОЇ СТІЙКОСТІ КАЛИНА-ПОДІБНИХ АЛГОРИТМІВ

Введемо необхідні позначення. Лінійний (над кільцем Z_{2^u}) оператор $A:(V_u)^p \to (V_u)^p$ задамо за допомогою матриці

$$A=\left(a_{ij}\right)_{i,j=1}^{p},\ a_{ij}\in V_u,$$

де для будь-якого $x=(x^{(p)},...,x^{(1)})\in V_n$:

$$A\,x^T=y^T=\left(y^{(p)},...,y^{(1)}\right)^T,\ y^{(i)}=\sum_{j=1}^{p}a_{ij}x^{(j)},$$

а операції множення та додавання виконуються у кільці Z_{2^u}. Позначимо $A_i=\left(a_{ip},...,a_{i1}\right)$. Тоді, в наших позначеннях, $y^{(i)}=A_i x^T$, тобто

$$A\,x^T=\left(A_p x^T,...,A_1 x^T\right)^T,$$

де під скалярним множенням розуміємо множення векторів з $\left(Z_{2^u}\right)^p$.

Аналогічно позначимо для оберненого оператора $A^{-1}=\left(A'_p,...,A'_1\right)$, де $A'_i,\ \ i=\overline{1,p}$ – рядки матриці A^{-1} (також пронумеровані у зворотному порядку, відповідно до нумерації координат вектора x). Тоді

$$A^{-1}x^T=\left(A'_p x^T,...,A'_1 x^T\right)^T.$$

Надалі розглядається лише такий оператор A, що для деякого фіксованого $l\in\mathbf{N}$: $wt\left(A'_j\right)\le l,\quad j=\overline{1,p}$.

Означення 2. В наших позначеннях називатимемо блоковий алгоритм шифрування (1) *модифікованим Калина-подібним алгоритмом,* якщо його раундова функція має вигляд:

$$f_k(x)=A\circ S(x*k),\qquad (9)$$

де $x\in V_n$ – відкритий текст, $n=pu,\ \ p\ge 2$, $x=(x_p,....,x_1)$, $x_i:V_u\to V_u$, $i=\overline{1,p}$, $k\in V_n$ – раундовий ключ, $*$ – операція побітового або модульного додавання, $S:V_n\to V_n$ – блок підстановки такий, що $S=(s^{(p)},...,s^{(1)})$, де $s^{(i)}:V_u\to V_u$.

Зазначимо, що модифікований зазначеним чином Калина-подібний алгоритм може містити:

1*) побітовий ключовий суматор;

2*) модульний ключовий суматор;

3*) операції модульного та побітового додавання чергуються в залежності від раунду.

Операція в ключовому суматорі і визначатиме властивості такого алгоритму.

Наступне твердження визначає для зазначених модифікованих Калина-подібних алгоритмів, чи є вони марковськими.

Лема 3. Залежно від ключового суматора модифікований Калина-подібний алгоритм з раундовою функцією (9) та ключовим суматором згідно з 1*)-3*) буде:

1*) марковським відносно операції побітового додавання $\oplus$ та узагальнено марковським відносно операції модульного додавання;

2*) марковським відносно операції модульного додавання + та узагальнено марковським відносно операції побітового додавання $\oplus$;

3*) узагальнено марковським відносно модульного і побітового додавання.

Доведення наведемо лише для 3*), оскільки інші пункти твердження доводяться безпосередньо, виходячи з аналогічних міркувань.

Розглянемо раундову функцію (9), позначимо її

$$f_k(x)=\varphi(x*k).$$

Для фіксованого $x\in V_n$ розглянемо вираз

$$2^{-n}\sum_{k\in V_n}\delta(f_k(x\circ_1\omega)\circ_2 f_k(x)^{-1},\omega')=$$

$$=2^{-n}\sum_{k\in V_n}\delta(\varphi((x\circ_1\omega)*k)\circ_2\varphi(x*k)^{-1},\omega').$$

Запишемо $x\circ_1\omega$ у такому вигляді: $x\circ_1\omega=\nu(x,\omega)*\omega*x$, де $\nu(x,\omega)=(x\circ_1\omega)*x^{-1}*\omega^{-1}$.

Зазначимо, що відображення $\omega\to\omega_0=\nu(x,\omega)*\omega$ при фіксованому $x\in V_n$ є перестановкою на V_n. Дійсно, якщо $\nu(x,\omega_1)*\omega_1=\nu(x,\omega_2)*\omega_2$, то

$$(x\circ_1\omega_1)*x^{-1}*\omega_1^{-1}*\omega_1=(x\circ_1\omega_2)*x^{-1}*\omega_2^{-1}*\omega_2,$$

звідки $x\circ_1\omega_1=x\circ_1\omega_2$, $\omega_1=\omega_2$.

Позначимо перестановку $\omega \to \nu(x,\omega) * \omega$ через $\sigma_x(\omega)$. З наведених вище міркувань випливає, що $\forall x \in V_n$:

$$2^{-n} \sum_{k \in V_n} \delta(\varphi((x \circ_1 \omega) * k) \circ_2 \varphi(x * k)^{-1}, \omega') =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(\varphi(\nu(x,\omega) * x * \omega * k) \circ_2 \varphi(x * k)^{-1}, \omega') =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(\varphi(\sigma_x(\omega) * k) \circ_2 \varphi_k(k)^{-1}, \omega'),$$

що й завершує доведення леми 3.

Твердження Леми 3 справедливе і у більш загальному випадку, а саме для такого шифру, у якого раундові функції мають вигляд $f_k(x) = \varphi(x * k)$, але є різними: наприклад, відрізняються операцією "*" у ключовому суматорі. У цьому випадку в твердження необхідно внести відповідні зміни щодо операції у ключовому суматорі.

Наступну лему можна вважати наслідком з Леми 3.

Лема 4. Для модифікованого Калина-подібного алгоритму з модульним ключовим суматором, справедлива така оцінка практичної стійкості до цілочисельного криптоаналізу:

$$EDP(\Omega) = \prod_{i=0}^{r-1} d_+^f(\omega_i, \omega_{i+1}).$$

Для побудови оцінок практичної стійкості модифікованих Калина-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу скористаємось наступними результатами з [16].

Теорема 3 ([16]) Нехай раундова функція має вигляд $f_k(x) = A \circ S(x+k)$. Тоді справедлива така нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\} \quad d_+^f(\alpha, \beta) \le \Delta_+,$$

де для кожного $i = \overline{1, p}$ покладемо

$$\Delta_+^{(i)} = \max_{\alpha, \gamma \in V_u \setminus \{0\}} \frac{1}{2^u} \sum_{k \in V_u} \left(\sum_{z=0}^{l+1} \delta\left(s^{(i)}(k+\alpha) - s^{(i)}(k), \gamma + z\right) \right) \quad (10)$$

та

$$\Delta_+ = \max\left\{\Delta_+^{(i)}, i = \overline{1, p}\right\}. \quad (11)$$

Теорема 4 ([16]) Нехай раундова функція має вигляд $f_k(x) = A \circ S(x \oplus k)$. Тоді справедлива наступна нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\} \quad d_+^G(\alpha, \beta) \le \Delta_{\oplus +},$$

де для кожного $l = \overline{1, p}$ визначено

$$\Delta_{\oplus +}^{(i)} = \max_{\alpha, \gamma \in V_n \setminus \{0\}} \frac{1}{2^u} \sum_{k \in V_u} \left(\sum_{z=0}^{l+1} \delta\left(S^{(i)}(k \oplus \alpha) - S^{(i)}(k), \gamma + z\right) \right) \quad (12)$$

та

$$\Delta_{\oplus +} = \max\left\{\Delta_{\oplus +}^{(i)}, i = \overline{1, p}\right\}. \quad (13)$$

Наведені теореми встановлюють верхні оцінки стійкості раундових функцій, визначених у (9). Зауважимо, що час обчислення величин $\Delta_{\oplus +}$ та Δ_+ для довжини входу k (розмір одного s-блоку) становить $O(lpk^3 \log k)$ бітових операцій.

Використовуючи результати лем 3 та 4, а також теорем 4 і 5, можна побудувати оцінки практичної стійкості для модифікованих алгоритмів «Калина» та «Кузнєчик» відносно цілочисельного різницевого криптоаналізу.

Теорема 5.

1) для модифікованого Калина-подібного алгоритму, верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \le \max_{\alpha, \beta \in V_n \setminus \{0\}} d_{+,+}^f(\alpha, \beta) \cdot \left(\max_{\alpha, \beta \in V_n \setminus \{0\}} d_{\oplus,+}^f(\alpha, \beta) \right)^{N-1},$$

де N – кількість раундів блокового алгоритму;

2) для модифікованого алгоритму «Кузнєчик», верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \le \max_{\alpha, \beta \in V_n \setminus \{0\}} d_{\oplus,+}^f(\alpha, \beta)^{N-1},$$

де N – кількість раундів блокового алгоритму.

Нижче наведено статистичний розподіл параметрів для 100000 вузлів заміни згенерованих випадковим чином.

Таблиця 5

Статистичний розподіл параметру (10) при $l = 8$ (вибірка з 100000 випадкових 8-бітових s-блоків)

Значення Δ_+	Значення $2^8 \cdot \Delta_+$	Кількість
0,08203125	21	19
0,0859375	22	2632
0,08984375	23	19230
0,09375	24	32814
0,09765625	25	24959
0,1015625	26	12627
0,10546875	27	4999
0,109375	28	1804
0,11328125	29	595
0,1171875	30	241
0,12109375	31	52
0,125	32	15
0,12890625	33	11
0,1328125	34	2

Таблиця 6

Статистичний розподіл параметру (12) при $l = 8$ (вибірка з 100000 випадкових 8-бітових s-блоків)

Значення $\Delta_{\oplus+}$	Значення $2^8 \cdot \Delta_{\oplus+}$	Кількість
0,08203125	21	5
0,0859375	22	789
0,08984375	23	8671
0,09375	24	22491
0,09765625	25	24806
0,1015625	26	18980
0,10546875	27	11004
0,109375	28	6396
0,11328125	29	3261
0,1171875	30	1807
0,12109375	31	862
0,125	32	465
0,12890625	33	230
0,1328125	34	126
0,13671875	35	61
0,140625	36	20
0,14453125	37	16
0,1484375	38	6
0,15234375	39	3
0,15625	40	1

На рисунку 1 подано значення з таблиці 6 у вигляді діаграми. Як бачимо, основна кількість s-блоків мають значення параметра (12) у межах від 0,08203125 до 0,16015625, причому найбільше s-блоків характеризуються значеннями 0,09765625, 0,09375 та 0,1015625. Отриманий розподіл параметру (12) зберігається і на 100 000 інших випадкових блоків нелінійної підстановки.

Отримані дані статистичних розподілів параметрів (10) та (12) дозволяють сприймати оцінки цих параметрів для s-блоків, визначених у національних стандартах для алгоритмів «Калина» та «Кузнєчик», у контексті загальної картини, характерної для s-блоків такого розміру.

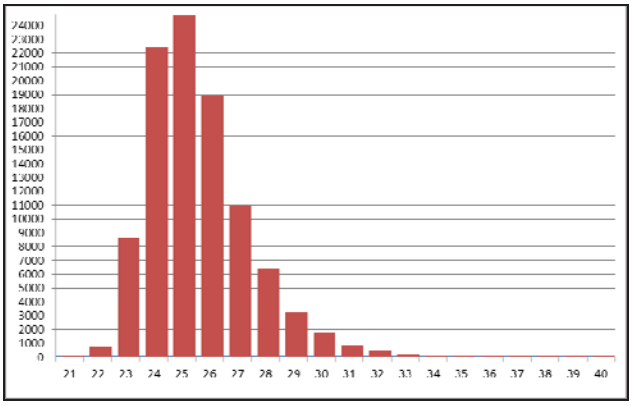

Рис.1

Використовуючи результати статистичного розподілу параметрів для $l = 8$ та восьмибітових s-блоків, зокрема, було знайдено підстановки з найменшими можливими значеннями цих параметрів, використання яких дозволить підвищити стійкість раундових перетворень по відношенню до цілочисельного різницевого криптоаналізу. Виходячи з отриманних результатів, верхні оцінки імовірностей цілочисельного раундового диференціалу для раундової функції (9) при відповідному виборі s-блоків, може приймати значення не більше 0,04 у випадку модульного ключового суматора та 0,05 побітового ключового суматора.

В таблиці 7 наведено статистичний розподіл параметрів для вузлів заміни, що рекомендовані в стандарті ДСТУ 7624:2014.

Таблиця 7

Статистичний розподіл параметрів (10), (11) восьмибітових вузлів заміни шифру ДСТУ 7624 («Калина»)

Підстановка	$\Delta_{+,+}$	$2^8 \cdot \Delta_{+}$
π_0	0,09765625	25
π_1	0,08984375	23
π_2	0,10546875	27
π_3	0,09375	24
${}_{-1}\pi_0$	0,11328125	29
${}_{-1}\pi_1$	0,08984375	23
${}_{-1}\pi_2$	0,10546875	27
${}_{-1}\pi_3$	0,09765625	25
max	0,11328125	29

Таблиця 8

Статистичний розподіл параметрів (12), та (13) восьмибітових вузлів заміни шифру ДСТУ 7624 («Калина»)

Підстановка	$\Delta_{\oplus+}$	$2^8 \cdot \Delta_{\oplus+}$
π_0	0,08984375	23
π_1	0,09375	24
π_2	0,0859375	22
π_3	0,09375	24
${}_{-1}\pi_0$	0,09375	24
${}_{-1}\pi_1$	0,08984375	23
${}_{-1}\pi_2$	0,09375	24
${}_{-1}\pi_3$	0,09375	24
max	0,09375	24

Використовуючи отримані дані, подані в таблицях 5–6, слід зауважити, що існує можливість обирати вузли заміни з такими значеннями параметрів, які забезпечуватимуть більшу стійкість Калина-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу.

В такому випадку, якщо вузли заміни обрані з рекомендованих в стандарті ДСТУ7624:2014 (див. таблиці 7 та 8), тоді $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta)\le 0{,}09375$ і $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}10546875$. Звідки, з урахуванням оцінки імовірності узагальненої диференціальної характеристики алгоритму з теореми 3 для 10 раундів зашифрування

$$EDP(\Omega)\le 5{,}9\cdot 10^{-11}\approx 2^{-34},$$

для 14 раундів зашифрування.

$$EDP(\Omega)\le 4{,}578\cdot 10^{-15}\approx 2^{-48},$$

для 18 раундів зашифрування

$$EDP(\Omega)\le 3{,}521\cdot 10^{-19}\approx 2^{-61}.$$

Якщо обрати вузли заміни, так щоб вони відповідали найменшим значенням параметрів (див. табл. 6) $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}08203125$ і $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}08203125$, у такому випадку для 10 раундів зашифрування отримали б $EDP(\Omega)\le 1{,}38\cdot 10^{-11}\approx 2^{-36}$ для 14 раундів зашифрування $EDP(\Omega)\le 6{,}248\cdot 10^{-16}\approx 2^{-51}$ і для 18 раундів зашифрування $EDP(\Omega)\le 2{,}829\cdot 10^{-20}\approx 2^{-65}$.

Для модифікованого алгоритму (з модульним ключовим суматором), при оптимальному виборі значень параметрів (див. таблицю 7) справедлива аналогічна оцінка.

В такому випадку, якщо використано вузол заміни із стандарту ГОСТ Р 34.12 2015, тоді для модифікованого алгоритму із побітовим додаванням у ключовому суматорі $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta)\le 0{,}0898437$, звідки за теоремою 3 для 10 раундів зашифрування (враховуючи, що останній раунд не використовує нелінійну заміну, а лише побітове додавання ключа), отримаємо $EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$.

Якщо розглянути модифікований алгоритм із операцією модульного додавання у ключовому суматорі, його практична стійкість оцінюється величинами $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}0898437$, для одного раунду зашифрування та за теоремою 3

$$EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$$

для 10 раундів шифрування.

ВИСНОВКИ

В даній статті отримано оцінки верхніх меж практичної стійкості модифікованого ГОСТ-подібного алгоритму та модифікованих алгоритмів «Кузнєчік» та «Калина» до цілочисельного різницевого криптоаналізу у двох випадках: коли у ключовому суматорі реалізована операція модульного додавання або побітового додавання. Наведені результати дозволяють оцінити практичну стійкість алгоритмів блокового шифрування визначених у стандартах України та Росії відносно цілочисельного різницевого криптоаналізу.

Порівняння значень отриманих параметрів зі статистичними розподілами випадкових параметрів дає привід припускати, що під час проектування шифру «Кузнєчік», окрім стійкості до класичного побітового різницевого криптоаналізу, могла бути врахована необхідність практичної стійкості і до цілочисельного різницевого криптоаналізу. Неможливо стверджувати напевно, чи був такий тип атаки розглянутий авторами шифру під час проектування його s-блоку. Слід зазначити, щодо інших сучасних алгоритмів, стійкість до цілочисельного різницевого криптоаналізу не розглядалася ні при побудові шифру AES, ні шифру «Калина». Якщо припущення – вірне, то «Кузнєчік» стає першим алгоритмом шифрування, який би використовував нелінійні вузли заміни за замовчуванням із близькими до практично досяжних найменших значень параметрів, тобто тих, що забезпечують йому практичну стійкість раундових перетворень до цілочисельного різницевого криптоаналізу. До того ж показники «Калини», хоч не на багато, але гірші, ніж «Кузнєчіка». Найгіршу стійкість до цілочисельного різницевого криптоаналізу з операцією побітового додавання в ключовому суматорі має третій s-блок «Калини», а до цілочисельного різницевого криптоаналізу з операцією модульного додавання в ключовому суматорі – другий. Але цей недолік було вирішено за допомогою збільшення кількості раундів шифрування.

Література

[1] СТБ 34.101-31.2011 Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности [Електронний ресурс] // Режим доступу: – http://apmi.bsu.by/assets/files/std/belt-spec27.pdf- Назва з екрану.

[2] ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.захисту інформації [Електронний ресурс] // Режим доступу: – http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf - Назва з екрану.

[3] ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Електронний ресурс] // Режим доступу: – https://eprint.iacr.org/2015/650.pdf - Назва з екрану.

[4] *Олексійчук А.М., Ковальчук Л.В., Пальченко С.В.* Криптографічні параметри вузлів заміни, що характеризу-

ють стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу. Захист інформації. – 2007, № 2. – С. 12 – 23.

[5] *Ковальчук Л. В., Пальченко С. В., Скрипник Л.В.* Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів до методів різницевого криптоаналізу. – Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2007, № 2 (16). – С. 70–84.

[6] *Ковальчук Л.* Обобщёные марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа. Труды Пятой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-06), 25-27 октября 2006. – С. 595–599.

[7] *Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л.* Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа. Труды Седьмой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-08), 30 октября – 2 ноября 2008. – С. 15–20.

[8] *X. Wang, H. Yu.* How to Break MD5 and Other Hash Functions. Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19–35.

[9] *S. Cotini, R.L. Riverst, M.J.B. Robshaw, Y. Lisa Yin.* Security of the RC6^{TM} Block Cipher, Режим доступу: – https://people.csail.mit.edu/rivest/ContiniRivestRobshawYin-TheSecurityOfTheRC6BlockCipher.pdf - Назва з екрану.

[10] *Tomas A.* Berson Differential cryptanalysis mod 2^{32} with applications to MD5. Advanced in Cryptology. – CRYPTO’98 (LNCS 372). – 1999. – P. 95–103.

[11] *Ковальчук Л.* Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. «Кибернетика и системный анализ» – 2010, №6, С. 89–96.

[12] *Ковальчук Л., Кучинская Н.* Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. «Кибернетика и системный анализ» – 2012, №5, С. 71–81.

[13] *Lai X.* Markov ciphers and differential cryptanalysis / X. Lai, J.L. Massey, S. Murphy. Advances in Cryptology – EUROCRYPT’91, Proceedings. – Springer Verlag, 1991. – pp. 17–38.

[14] *Алексейчук А. Н. Ковальчук Л.В.* Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю 2^m . Прикладная радиоэлектроника. – 2006. – Т. 5, № 1. – С. 74–82.

[15] *Кучинская Н. В., Скрипник Л.В* Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига. Спеціальні телекомунікаційні системи та захист інформації. – 2013. – Вип. 2(24). – С.26–32.

[16] *Ковальчук Л., Кучинська Н., Скрипник Л.* Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора . Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2015. – №1(29). – С.33–45.

[17] Наказ Адміністрації Держспецзв'язку №114 Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації Редакція від 27.06.2013 [Електронний ресурс] // Режим доступу: – http://zakon3.rada.gov.ua/laws/show/z0729-07 - Назва з екрану.

Надійшла до редколегії 29.12.2017

Ковальчук Людмила Василівна, доктор технічних наук, професор, професор кафедри математичних методів захисту інформації, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського, область наукових інтересів: сучасні методи криптоаналізу блокових алгоритмів шифрування, методи аналізу якості псевдовипадкових послідовностей, сучасні асиметричні криптосистеми та методи їх криптоаналізу, криптовалюти.

Кучинська Наталія Вікторівна, кандидат технічних наук, доцент кафедри інформаційної безпеки, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського, область наукових інтересів: сучасні методи криптоаналізу блокових алгоритмів шифрування, методи аналізу якості псевдовипадкових послідовностей.

УДК 681.3.06:006.354

Оценки практической стойкости модифицированных стандартов блокового шифрования Украины и России относительно целочисленного разностного криптоанализа / Л.В. Ковальчук, Н.В. Кучинская // Прикладная радиоэлектроника: науч.-техн. журнал. – 2017. – Том 16, № 3, 4 – С. 155–165.

Рассмотрено одну из модификаций разностного криптоанализа, а именно целочисленный разностный криптоанализ. В статье получены научно-обоснованные оценки практической стойкости к целочисленному разностному криптоанализу модифицированных стандартов блочного шифрования Украины и России. Представлено зависимость полученных оценок от параметров, которые характеризуют s-блоки. Проведено сравнительный анализ значений этих параметров для всех алгоритмов, рассмотренных в работе. Также представлено статистическое распределение полученных параметров по случайной выборке из 100000 s-блоков.

Ключевые слова: разностный криптоанализ, стандарты блочного шифрования, s-блоки.

Табл.: 08. Рис.: 01. Библиогр.: 17 наим.

UDC 681.3.06:006.354

Estimates of the practical stability of the modified block encryption standards of Ukraine and Russia with respect to integer difference cryptanalysis / L.V. Kovalchuk, N.V. Kuchinska // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 155–165.

One of the differential cryptanalysis modifications is considered, namely, the integer differential cryptanalysis. The paper provides scientifically grounded estimates of practical security to integer differential cryptanalysis of the block encryption modified standards of Ukraine and Russia. The dependence of the obtained estimates on the parameters that characterize s-blocks is presented. A comparative analysis of values of these parameters for all the algorithms considered in the work is carried out. A statistical distribution of the obtained parameters is also presented for a random sample of 100,000 s-blocks

Keywords: difference cryptanalysis, block encryption standards, s-blocks.

Tab.: 08. Fig.: 01. Ref.: 17 items.