Викулов Павел Александрович, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
Email: p.vikulov@ukr.net
Вікулов Павло Олександрович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
Vikulov Pavlo, PhD student of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Шаховал Александра Анатольевна, старший лаборант кафедры безопасности информационных технологий Национального авиационного университета.
Email: shakhoval.al@gmail.com
Шаховал Олександра Анатоліївна, старший лаборант кафедри безпеки кафедри безпеки інформаційних технологій Національного авіаційного університету.
Shakhoval Oleksandra, senior laboratory assistant of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.19.11903
УДК 003.26:004.056.55

КРИПТОГРАФІЧНИЙ МЕТОД ЗАХИСТУ КРИТИЧНИХ АВІАЦІЙНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сергій Гнатюк, Василь Кінзерявий, Берік Ахметов, Каріна Кириченко, Кирило Ануфрієнко

Забезпечення конфіденційності даних є важливим етапом у процесі забезпечення кібербезпеки критичних авіаційних інформаційних систем та авіаційної галузі у цілому. Відомі методи не дозволяють у повній мірі забезпечити стійкість до кібератак лінійного та диференціального криптоаналізу і необхідну швидкість криптографічної обробки даних. З огляду на це, у роботі розроблено криптографічний метод захисту критичних авіаційних інформаційних систем. На основі даного методу побудовано блоковий симетричний шифр Lmna-2k17 та у роботі наведена специфікація даного шифру. Також, розраховано значення верхніх оцінок параметрів, що характеризують його практичну стійкість до кібератак лінійного та диференціального криптоаналізу. За однакових умов, проведені експериментальні дослідження з оцінки швидкісних характеристик шифрів, які показали, що шифр Lmna-2k17 швидший за шифр ГОСТ 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази.
Ключові слова: *криптографія, блоковий шифр, лінійний криптоаналіз, диференціальний криптоаналіз, захист інформації.*

Вступ. Цивільна авіація є галуззю критичної інфраструктури держави, внутрішнє середовище якої швидко і суттєво змінюється із впровадженням сучасних інформаційно-комунікаційних технологій. Відповідно до керівних документів у галузі цивільної авіації найбільшого захисту потребують критичні авіаційні інформаційні системи (КАІС) [1], до яких згідно [2] відносяться, наприклад, системи управління повітряним рухом, системи дистанційного технічного обслуговування, диспетчерські системи та ін. Для мінімізації впливу кіберзагроз на ресурси КАІС необхідно вжити низку заходів [3], серед яких забезпечення конфіденційності даних (інформації). Одним із найважливіших напрямів діяльності щодо забезпечення конфіденційності даних був і залишається захист інформації криптографічними методами [4], беззаперечною перевагою яких є забезпечення захисту безпосередньо самих даних, а не доступу до них. Основним критерієм при виборі криптосистем є стійкість, проте для деяких завдань ключову роль відіграє швидкість криптографічної обробки даних [4-5]. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту даних, а розвиток і здешевлення інформаційно-комунікаційних технологій позитивно впливає на ефективність криптоаналізу, одними з найефективніших методів якого є лінійний та диференціальний криптоаналіз [6-8].

Постановка завдання. Таким чином, розробка криптографічного методу захисту КАІС та обґрунтування його ефективності є *актуальним* науковим завдання. Зважаючи на це, *метою роботи* є підвищення ефективності криптографічного захисту КАІС на базі розробки нового

криптографічного методу захисту даних та відповідного блокового шифру на його основі.

Опис розробленого криптографічного методу захисту КАІС. Нехай t', p', r', q' – натуральні числа, $t=2t'$, $p=2p'$, $r=2r'+1$, $n=tp$, $q=pq'$, $w=p$, $k=2n$, $b=2^{q'}$ (параметр b визначає кількість різних таблиць замін (підстановок), що можуть використовуватись у методі). Тоді r-раундовий метод криптографічного захисту КАІС $\Im$ із множиною відкритих (шифрованих) повідомлень $V_n=\{0,1\}^n$, множиною секретних ключів V_k, множиною раундових ключів V_{n+q+w} можна описати такою послідовністю етапів:

<u>Етап 1 – Вироблення раундових ключів</u>. На цьому етапі із секретного ключа K, $K\in V_k$ виробляється r раундових ключів K_i, $K_i\in V_{n+q+w}$, $i=\overline{1,r}$.

Крок 1. Секретний ключ K, $K\in V_k$ розкладається на частини:

$$K=\left(B_{-4},B_{-3},B_{-2},B_{-1}\right), \quad (1)$$

$B_j\in V_{n/2}$, $j=\overline{-4,-1}$.

Крок 2. Виробляються вектори $B_j, B_j\in V_{n/2}$, $j=\overline{0,c-1}$, $c=\lceil 4r(n+q+w)/n\rceil$:

$$B_j=\begin{cases}\left(S\left(B_{j-4},W_1,p'\right)\oplus\left(B_{j-2}<<<P_1\right)\oplus B_{j-1}\oplus Q_1\right)<<<B_{j-3} & ,\ j \bmod 4=0\\ \left(S\left(B_{j-3}\oplus B_{j-1},W_2,p'\right)\oplus\left(B_{j-2}>>>P_2\right)\oplus Q_2\right)>>>B_{j-4} & ,\ j \bmod 4=1\\ \left(B_{j-4}\oplus\left(S\left(B_{j-3}\right)<<<P_3,W_3,p'\right)\oplus B_{j-1}\oplus Q_3\right)>>>B_{j-2} & ,\ j \bmod 4=2\\ \left(S\left(B_{j-4}<<<P_4,W_4,p'\right)\oplus B_{j-3}\oplus B_{j-2}\oplus Q_4\right)<<<B_{j-1} & ,\ j \bmod 4=3\end{cases}, \quad (2)$$

де $\oplus$ – операція покоординатного булевого додавання двійкових векторів, $X<<<Y$ – операція динамічного циклічного зсуву вліво бітової послідовності X на Y разів, а $X>>>Y$ – операція динамічного циклічного зсуву вправо бітової послідовності X на Y разів, W_i, P_i, Q_i – деякі константи, $W_i,\ P_i,\ Q_i\in V_{n/2}$, $i=\overline{1,4}$.

Підстановка S визначаються за формулою:

$$S(x,y,z)=\left(s_{y_{z-1}}(x_{z-1}),\dots,s_{y_0}(x_0)\right),$$
$$x=(x_{z-1},\dots,x_0),\ y=(y_{z-1},\dots,y_0), \quad (3)$$

де $x_j\in V_t$, $y_j\in V_{q'}$, s_{y_j} – таблиця замін на множині V_t (за індексом y_j обирається для використання одна таблиця замін із b можливих), $j\in\overline{0,z-1}$.

Крок 3. Формуються вектори $C_i, C_i\in V_e$, $i=\overline{1,r}$, $e=e'n/2$, $e'=\lceil 2(n+q+w)/n\rceil$ конкатенацією векторів $B_j, B_j\in V_{n/2}$, $j=\overline{0,c-1}$, $c=\lceil 4r(n+q+w)/n\rceil$ у зворотному порядку (для формування одного вектора C_i використовується e' векторів B_j):

$$C_i=\left(B_{c-1-(i-1)e'}\,\|\,B_{c-1-(i-1)e'-1}\,\|\dots\|\,B_{c-1-(i-1)e'-e'+1}\right). \quad (4)$$

Крок 4. Розраховуються раундові ключі K_i, $K_i\in V_{n+q+w}$, $i=\overline{1,r}$:

$$K_i=\left(C_i>>>i\right)\bmod 2^{n+q+w}. \quad (5)$$

Отримані раундові ключі K_i, $K_i\in V_{n+q+w}$, $i=\overline{1,r}$ будуть використовуватись при шифруванні чи розшифруванні секретного повідомлення.

<u>Етап 2 – Процедура шифрування</u>. На цьому етапі відбувається шифрування секретного повідомлення $\grave{A}=\left(A_1,A_2,A_3,\dots,A_u\right)$, $\grave{A}\in V_{n\cdot u}$, $\grave{A}_j\in V_n$, $j=\overline{1,u}$, u – натуральне число.

Функція шифрування кожного $\grave{A}_j\in V_n$, $j=\overline{1,u}$ буде такою:

$$F=f_{r,K_r}\circ\dots\circ f_{1,K_1}. \quad (6)$$

Раундова функція f_{i,K_i}, для будь-яких $x\in V_n$, $K_i\in V_{n+q+w}$, $i\in\overline{1,r}$ описується наступним чином:

$$f_{i,K_i}(x)=\begin{cases}\varphi\left(x\oplus k^{(1)},k^{(2)},k^{(3)}\right), & якщо\ \ i<r\\ S\left(x\oplus k^{(1)},k^{(2)},p\right), & якщо\ \ i=r\end{cases}, \quad (7)$$

де $k^{(1)}$, $k^{(2)}$, $k^{(3)}$ частини раундового ключа K_i ($k=\left(k^{(1)},k^{(2)},k^{(3)}\right)$, $k^{(1)}\in V_n$, $k^{(2)}\in V_q$, $k^{(3)}\in V_w$).

Підстановка S визначена у (3), а підстановка φ визначається за формулою:

$$\varphi(x, y, h) = S(x, y, p)M(h),$$
$$x \in V_n,\ y \in V_q,\ h \in V_w, \quad (8)$$

де $x = (x_{p-1}, \dots, x_0), y = (y_{p-1}, \dots, y_0)$, $x_j \in V_t$, $y_j \in V_{q'}$.

$M(h)$ – оборотна $2p \times 2p$ матриця над полем $GF(2^{t'})$, що залежить від h, а множення $S(x, y, p) = (s_{y_{p-1}}(x_{p-1}), \dots, s_{y_0}(x_0))$ на $M(h)$ у (8) виконується над цим полем таким чином:

1. $s_{y_j}(x_j)$ ($j \in \overline{0, p-1}$) розкладається на дві t'-бітні частини

$$(s_{y_j}(x_j) = (s_{y_j}(x_j)^{(1)}, s_{y_j}(x_j)^{(2)}),$$
$$s_{y_j}(x_j)^{(1)}, s_{y_j}(x_j)^{(2)} \in V_{t'}).$$

2. Із частин $s_{y_j}(x_j)$ ($j \in \overline{0, p}$) формується вектор B:

$$B = s_{y_0}(x_0^{(1)}) || s_{y_0}(x_0^{(2)}) || \dots ||$$
$$s_{y_{p-1}}(x_{y_{p-1}}^{(1)}) || s_{y_{p-1}}(x_{y_{p-1}}^{(2)}).$$

3. Виконується множення вектора B на $M(h)$ при ототожненні двійкових векторів B_j $j \in \overline{0, 2p-1}$ ($B_j \in V_{t'}$) із елементами матриці $M(p)$.

На основі робіт [9, 10], для запропонованого методу отримано аналітичні верхні оцінки параметрів, що характеризують його практичну стійкість відносно методів лінійного та диференціального криптоаналізу:

$$EDP(\Omega) \le \tilde{\Delta}_{\oplus}^{r'\lceil B_M/2\rceil+1} \le \Delta_{\oplus}^{r'\lceil B_M/2\rceil+1}, \quad (9)$$

$$ELP(\Omega) \le \tilde{\Lambda}_{\oplus}^{r'\lceil B_M/2\rceil+1} \le \Lambda_{\oplus}^{r'\lceil B_M/2\rceil+1}, \quad (10)$$

де $EDP(\Omega)$ – середня імовірність диференціальної характеристики Ω, $ELP(\Omega)$ – середня імовірність лінійної характеристики Ω, B_M – індекс галуження матриці M, а параметри $\Delta_{\oplus}$, $\Lambda_{\oplus}$, $\tilde{\Delta}$, $\tilde{\Lambda}$ визначаються за формулами:

$$\Delta_{\oplus} = \max\left\{d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \quad (11)$$

$$\Lambda_{\oplus} = \max\left\{l^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \quad (12)$$

$$\tilde{\Delta}_{\oplus} = \max\left\{b^{-1}\sum_{j=0}^{b-1} d_{\oplus}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}\right\}, \quad (13)$$

$$\tilde{\Lambda}_{\oplus} = \max\left\{b^{-1}\sum_{j=0}^{b-1} l^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}\right\}. \quad (14)$$

У (11) – (14) $d_{\oplus}^{(s_j)}$ – таблиця різниць підстановки s_j ($j \in \overline{0, b-1}$) відносно операцій побітового додавання за модулем 2, а $l^{(s_j)}(\alpha, \beta)$ – таблиці лінійної апроксимації підстановки s_j ($j \in \overline{0, b-1}$) відносно цієї самої операції.

Блоковий шифр Luna-2k17. На основі запропоновано методу розроблено БШ Luna-2k17.

Для даного шифру обрано такі параметри: $t' = 8$, $t = 2t' = 16$ (розрядність таблиць замін), $p' = 4$, $p = 2p' = 8$, $r' = 4$, $r = 2r' + 1 = 9$ (кількість раундів), $n = tp = 128$ (розмір блоку даних, біт), $q' = 3$, $q = pq' = 24$, $b = 2^{q'} = 8$ (використовується 8 таблиць замін на множині V_{16}), $w = 8$, $k = 2n = 256$ (розмір секретного ключа, біт).

Запропонований шифр працює із 128-бітними блоками даних з підтримкою секретного ключа довжиною 256 біт. При розширенні секретного ключа виробляється необхідна кількість 160-бітних раундових ключів $(n + q + w = 128 + 24 + 8 = 160)$. Блоки даних та розширені ключі представляються у вигляді 8×2 байтної матриці.

Для шифру Luna-2k17 *процедура вироблення раундових ключів* виконується за формулами (1)-(5). У кроці один 256 бітний раундовий ключ K розбивається на 4 частини: $K = (B_{-4}, B_{-3}, B_{-2}, B_{-1})$, довжиною 64 біти кожна. Далі на кроці два розраховуються допоміжні 64-бітні вектори B_j, $j = \overline{0, 44}$ ($c = \lceil 4r(n+q+w)/n \rceil = 4 \cdot 9 \cdot (128 + 24 + 8)/128 = 45$).

При цьому використовуються 64-бітні константи W_i, P_i, Q_i, $i = \overline{1, 4}$. У табл. 1 наведено значення даних констант.

Також у кроці два у підстановці S використовуються 8 таблиць замін 16 на 16 біт. Дані таблиці замін побудовані за допомогою обрахунку зворотного елементу поля $(C / X)^{-1} \in GF(2^{16})$ з подальшим виконанням афінного перетворення над полем $GF(2)$:

$$S(X) = M \cdot (C / X)^{-1} + V, \qquad (15)$$

де $X, C, V \in GF(2^{16})$, а M – квадратна не вироджена матриця над полем $GF(2)$ розміром 16×16.

Параметри C, V та M наведені в шістнадцятеричному вигляді в табл. 2 (кожний рядок матриці M відображений у вигляді одного шістнадцятеричного числа).

Таблиця 1

Значення 64-бітних констант, що використовуються у БШ

Константа	**Значення константи у шістнадцятковій системі числення**
W_1	E702 DDCB BDEC BDD5
W_2	4AB4 2988 9FE1 017A
W_3	7BED 569B 1C78 2259
W_4	15A7 5069 7EF5 439C
P_1	89FC BB23 4DB0 D712
P_2	1970 CB03 479F E7B2
P_3	2FA8 934D EB78 0517
P_4	07C4 20F9 87D1 0ECA
Q_1	8713 DC71 F897 4562
Q_2	D896 3354 4110 80BA
Q_3	5CB1 AE69 0140 DB83
Q_4	A09B E122 36B4 C17A

Таблиця 2

Параметри C, V та M, що були використані для побудови таблиць замін на множині V_{16}

Інд. табл. замін	***M***	***C***	***V***
0	{0652,0CA4,1948,3290,6520,CA40,9481,2903,5206,A40C,4819,9032,2065,40CA,8194,0329}	06FB	09F0
1	{32ED,65DA,CBB4,9769,2ED3,5DA6,BB4C,7699,ED32,DA65,B4CB,6997,D32E,A65D,4CBB,9976}	6A8C	760E
2	{32F0,65E0,CBC0,9781,2F03,5E06,BC0C,7819,F032,E065,C0CB,8197,032F,065E,0CBC,1978}	7992	200B
3	{32FA,65F4,CBE8,97D1,2FA3,5F46,BE8C,7D19,FA32,F465,E8CB,D197,A32F,465F,8CBE,197D}	01AC	1E00
4	{3975,72EA,E5D4,CBA9,9753,2EA7,5D4E,BA9C,7539,EA72,D4E5,A9CB,5397,A72E,4E5D,9CBA}	7AE3	6EDF
5	{3985,730A,E614,CC29,9853,30A7,614E,C29C,8539,0A73,14E6,29CC,5398,A730,4E61,9CC2}	697C	40CD
6	{3B2B,7656,ECAC,D959,B2B3,6567,CACE,959D,2B3B,5676,ACEC,59D9,B3B2,6765,CECA,9D95}	4724	68FD
7	{3C54,78A8,F150,E2A1,C543,8A87,150F,2A1E,543C,A878,50F1,A1E2,43C5,878A,0F15,1E2A}	02EE	75D5

На третьому кроці формуються 192-бітні вектори C_i, $C_i \in V_{192}$, $i = \overline{1,9}$ ($e' = \lceil 2(n+q+w)/n \rceil = 3$, $e = e'n/2 = 192$). Далі на четвертому кроці формуються 160-бітні раундові ключі K_i, $i = \overline{1,9}$.

Для шифру Luna-2k17 *процедура зашифровування* виконується за формулами (6)-(8). На рис. 1. наведено псевдокод процедури зашифровування.

Під операцією $AddKeyMod2(state, SubKey^{(1)})$ мається на увазі побітове додавання за модулем 2 відповідних бітів раундового ключа $SubKey^{(1)}$ та блоку данних $state$.

Операція $MixColumns(state)$ являє собою лінійне перетворення матриці $state$. У даній операції кожна 8-байтна колонка блоку данних $state$ розглядається як поліном над полем

$GF\left(2^8\right)$ з 8 термами, який перемножується за модулем x^8+1 з фіксованим поліномом $c(x)$ степені 7. У якості поліному $c(x)$ обраний наступний поліном: $c(x)=3x^7+7x^6+x^5+3x^4+7x^3+4x^2+1Dx+1$ (коефіцієнти представлені в 16-ричній формі). У якості незвідного многочлена, був обраний многочлен: $m(x)=x^8+x^7+x^5+x^4+x+1$.

Luna-2k17 Процедура зашифрування

Input: 128-бітний вхідний блок даних $state$, 160-бітні раунд. ключі

$$SubKey_i=\left(SubKey_i^{(1)},SubKey_i^{(2)},SubKey_i^{(3)}\right),\quad i=\overline{0,\mathrm{r}},\ SubKey_i^{(1)}\in V_{128},\ SubKey_i^{(2)}\in V_{24},\ SubKey_i^{(3)}\in V_8.$$

Output: 128-бітний вихідний блок даних $state$.

1. $state=AddKeyMod2\left(state,SubKey_0^{(1)}\right);$
2. $For\quad i=1,\quad i<r,\quad i++\quad do$
2.1. $state=SubBytes\left(state,SubKey_i^{(2)},8\right);$
2.2. $state=ShiftRows\left(state,SubKey_i^{(3)}\right);$
2.3. $state=MixColumns\left(state\right);$
2.4. $state=AddKeyMod2\left(state,SubKey_i^{(1)}\right);$
3. $state=SubBytes\left(state,SubKey_r^{(2)},8\right);$
4. $state=ShiftRows\left(state,SubKey_r^{(3)}\right);$
5. $state=AddKeyMod2\left(state,SubKey_r^{(1)}\right);$
6. $return\ state$.

Рис. 1. Псевдокод процедури зашифровування БШ Luna-2k17

В операціях $SubBytes\left(state,SubKey^{(2)},8\right)$ виконується таблична заміна кожних 16 біт блоку даних $state$. У шифрі Luna-2k17 використовуються 8 таблиць на множині V_{16}, при чому вибір конкретної таблиці у кожному раунді залежить від частини раундового ключа $SubKey^{(2)}$ згідно формули (3).

Таблиці замін були згенеровані згідно формули (15), параметри C, V та M, що використовувались при генеруванні наведені у табл. 2. Дані таблиці замін обрані таким чином, щоб були відсутні фіксовані точки, а також щоб виконувалися рівності для параметрів: $\Delta_{\oplus}=\Lambda_{\oplus}=2^{-14}$ – для кожної таблиці замін шифру Luna-2k17.

В операції $ShiftRows\left(state,SubKey^{(3)}\right)$ виконується побайтовий зсув елементів у рядках матриці $state$ в залежності від частини раундового ключа $SubKey^{(3)}$. Довжина частини раундового ключа $SubKey^{(3)}$ всього 8 біт, тому кожен біт даного вектора впливає на зсув відповідного рядка матриці $state$. Наприклад, якщо перший біт вектор $SubKey^{(3)}$ дорівнює 1, тоді значення стовпців 1-го рядка матриці $state$ переставляються місцями, якщо ж перший біт вектор $SubKey^{(3)}$ дорівнює 0, тоді значення стовпців 1-го рядка залишаються без змін.

На рис. 2. наведено псевдокод *процедури розшифровування*.

Luna-2k17 Процедура розшифрування

Input: 128-бітний вхідний блок даних $state$, 160-бітні раунд. ключі

$$SubKey_i=\left(SubKey_i^{(1)},SubKey_i^{(2)},SubKey_i^{(3)}\right),\quad i=\overline{0,\mathrm{r}},\ SubKey_i^{(1)}\in V_{128},\ SubKey_i^{(2)}\in V_{24},\ SubKey_i^{(3)}\in V_8.$$

Output: 128-бітний вихідний блок даних $state$.

1. $state=AddKeyMod2\left(state,SubKey_r^{(1)}\right);$
2. $For\quad i=1,\quad i<r,\quad i++\quad do$
2.1. $state=ShiftRows\left(state,SubKey_{r-i+1}^{(3)}\right);$
2.2. $state=InvSubBytes\left(state,SubKey_{r-i+1}^{(2)}\right);$
2.3. $state=AddKeyMod2\left(state,SubKey_{r-i}^{(1)}\right);$
2.4. $state=InvMixColumns\left(state\right);$
3. $state=ShiftRows\left(state,SubKey_1^{(3)}\right);$
4. $state=InvSubBytes\left(state,SubKey_1^{(2)}\right);$
5. $state=AddKeyMod2\left(state,SubKey_0^{(1)}\right);$
6. $return\ state$.

Рис. 2. Псевдокод процедури розшифровування БШ Luna-2k17

Операція $InvMixColumns\left(state\right)$ являє собою лінійне перетворення матриці $state$ – зворотне до $MixColumns\left(state\right)$. У даній операції кожна 8-байтна колонка блоку данних $state$ розглядається як поліном над полем $GF\left(2^8\right)$ з 8 термами, який

перемножується за модулем x^8+1 з фіксованим поліномом $d(x)$ степені 7. У якості поліному $d(x)$ обраний наступний поліном: $d(x)=7Ax^7+A1x^6+F8x^5+EEx^4+29x^3+89x^2+EBx+51$ (коефіцієнти представлені в 16-ричній формі).

В операції $InvSubBytes(state, SubKey^{(2)})$ виконується таблична заміна кожних 16 біт блоку даних $state$. Дана операція зворотна до $SubBytes(state, SubKey^{(2)})$, тому у ній використовуються зворотні таблиці замін порівняно із таблицями $SubBytes(state, SubKey^{(2)})$.

Експериментальні дослідження блокового шифру Luna-2k17.

Для експериментального дослідження блоковий шифр Luna-2k17 був програмно реалізований у вигляді консольного застосунку «Luna-2k17».

Статистичні властивості послідовностей, утворених за допомогою цього застосунку (у режимі лічильника) досліджено у середовищах статистичних тестів NIST STS. Статистичні портрети блоковим шифром Luna-2k17 наведено на рис. 3. У табл. 3 для порівняння наведено результати тестування послідовностей, сформованих шифрами Luna-2k17, ГОСТ 28147-89, Калина, AES. Як видно з результатів, шифр Luna-2k17 пройшов комплексний контроль за методиками NIST STS та показав не гірші результати ніж вище зазначені шифри.

Також досліджені *швидкісні характеристики* шифрів. Експериментально показано, що шифр Luna-2k17 швидший за шифр ГОСТ 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази (див. табл. 4). Дослідження проводилися в однакових умовах на Intel (R) Core (TM) i7-2600K CPU 3.4 GHz.

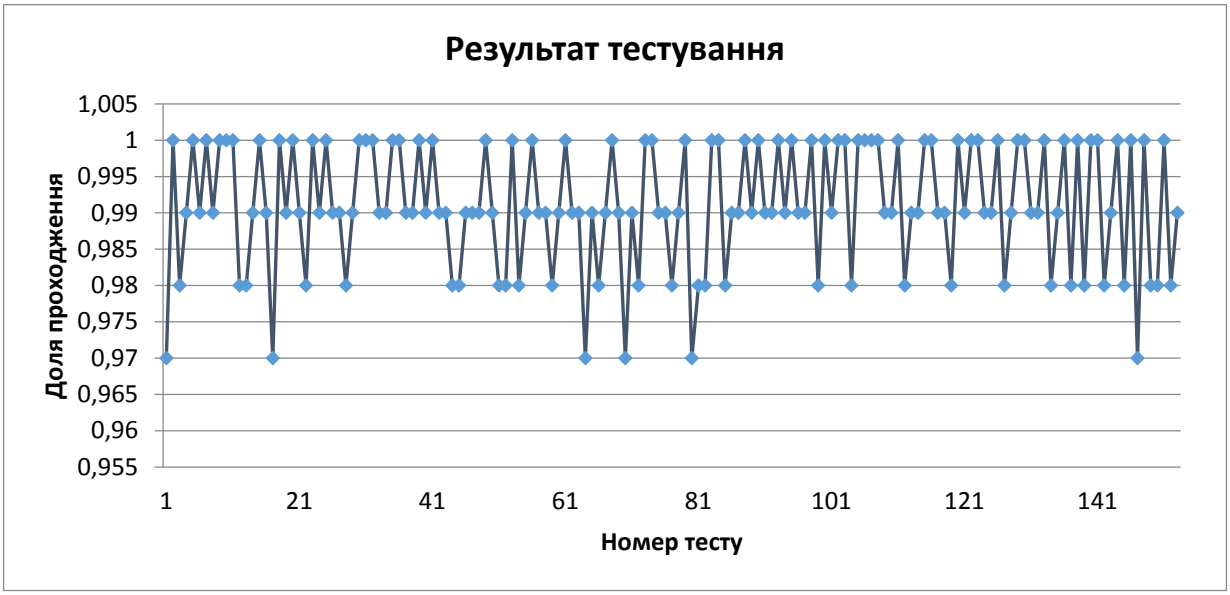

Рис. 3. Результати тестування БШ Luna-2k17 у середовищах статистичних тестів NIST STS

Таблиця 3

Результати тестування послідовностей за методикою NIST STS

Генератор	Кількість тестів, у яких тестування пройшло	
	99% послід.	96% послід.
BBS	132 (70,2%)	188 (100%)
Калина	137 (72,9%)	188 (100%)
ГОСТ 28147-89	130 (69,1%)	186(98,9%)
AES	133 (70,7%)	188 (100%)
Luna-2k17	141 (75,0%)	188 (100%)

Таблиця 4

Порівняння швидкісних характеристик блокових шифрів

БШ	Швидкість шифрування (МБ/с)
AES -256	64,93
Калина -256	71,19
ГОСТ 28147-89	29,02
Luna-2k17	90,48

Також розраховані *оцінки стійкості* шифру Luna-2k17 відносно методів лінійного та диференціального криптоаналізу. Згідно формул (9) – (14) розраховано значення верхніх оцінок параметрів, що характеризують практичну стійкість блокового шифру Luna-2k17 відносно методів лінійного та диференціального криптоаналізу: при $\Delta_{\oplus} = \Lambda_{\oplus} = 2^{-14}$, $r' = 4$, $B_M = 9$ – $EDP(\Omega) \le 2^{-294}$, $ELP(\Omega) \le 2^{-294}$ при кількості раундів $r = 9$. Це свідчить, що при $r \ge 9$ буде забезпечено практичну стійкість шифру Luna-2k17 відносно зазначених методів криптоаналізу.

Висновки. Таким чином, розроблено криптографічний метод захисту КАІС, який за рахунок нової послідовності операцій в процедурах вироблення раундових ключів та шифрування (використовуються таблиці замін із збільшеною розрядністю та рандомізуються лінійні і не лінійні операції) дозволяє підвищити ефективність криптографічного захисту КАІС. На основі даного методу побудовано блоковий симетричний шифр Luna-2k17. Розраховано значення верхніх оцінок параметрів, що характеризують його практичну стійкість до кібератак лінійного та диференціального криптоаналізу. За однакових умов, проведені експериментальні дослідження з оцінки швидкісних характеристик шифрів, які показали, що шифр Luna-2k17 швидший за шифр ГОСТ 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази. Також, досліджено статистичні властивості послідовностей сформованих блоковим шифром Luna-2k17, в результаті показано, що шифр Luna-2k17 пройшов комплексний контроль за методиками NIST STS та показав не гірші результати ніж інші шифри.

ЛІТЕРАТУРА

[1]. S. Gnatyuk, "Critical Aviation Information Systems Cybersecurity", *Meeting Security Challenges Through Data Analytics and Decision Support*. NATO Science for Peace and Security Series. D: Information and Communication Security. IOS Press Ebooks, vol. 47, no. 3, pp. 308-316, 2016.

[2]. С. Гнатюк, Д. Васильєв, "Сучасні критичні авіаційні інформаційні системи", *Безпека інформації,* Т. 22, №1, С. 51-57, 2016.

[3]. K. Janisz, O. Korchenko, S. Gnatyuk, R. Odarchenko, "Model for Cybersecurity Requirements Definition in Civil Aviation", *Autobusy*, no. 12, pp. 630-634, 2016.

[4]. С. Гнатюк, В. Кінзерявий, А. Охріменко, "Особливості криптографічного захисту державних інформаційних ресурсів", *Безпека інформації*, №1 (17), С. 64-77, 2012.

[5]. О. Корченко, С. Гнатюк, Ю. Хохлачова, А. Охріменко, "Основні критерії та вимоги до побудови сучасних криптосистем", *Вісник Інженерної академії України*, №3-4, С. 77-83, 2011.

[6]. E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology,* vol. 4, no. 1, pp. 3-72, 1991.

[7]. X. Lai, J.L. Massey, S. Murphy, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology. EUROCRYPT'91. Proceedings. Springer Verlag*, pp. 17-38, 1991.

[8]. M. Matsui, "Linear cryptanalysis methods for DES cipher", *Advances in Cryptology. EUROCRYPT'93. Proceedings. Springer Verlag*, pp. 386-397, 1994.

[9]. А. Алексейчук, Л. Ковальчук, Е. Скрынник, А. Шевцов, "Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах", *Прикладная радиоэлектроника*, Т. 7, №3, С. 203-209, 2008.

[10]. В. Кінзерявий, "Верхні оцінки стійкості блокових шифрів із рандомізованими вузлами замін до методів лінійного та диференціального криптоаналізу", *Захист інформації*, Т. 15, № 1,С. 21–31, 2013.

REFERENCES

[1]. S. Gnatyuk, "Critical Aviation Information Systems Cybersecurity", *Meeting Security Challenges Through Data Analytics and Decision Support*. NATO Science for Peace and Security Series. D: Information and Communication Security. IOS Press Ebooks, vol. 47, no. 3, pp. 308-316, 2016.

[2]. S. Gnatyuk, D. Vasiliev, "Modern critical aviation information systems", *Information security*, vol. 22, no. 1, pp. 51-57, 2016.

[3]. K. Janisz, O. Korchenko, S. Gnatyuk, R. Odarchenko, "Model for Cybersecurity Requirements Definition in Civil Aviation", *Autobusy*, no. 12, pp. 630-634, 2016.

[4]. S. Gnatyuk, V. Kinzeryavyy, A. Ohrimenko, "Specifics of cryptographic protection of state information resources", *Information security,* no. 1 (17), pp. 64-77, 2012.

[5]. O. Korchenko, S. Gnatyuk, Y. Hohlacheva, A. Ohrimenko, "The main criteria and requirements for the construction of modern cryptosystems", *Bulletin of the Engineering Academy of Ukraine,* no. 3-4, pp. 77-83, 2011.

[6]. E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology,* vol. 4, no. 1, pp. 3-72, 1991.

[7]. X. Lai, J.L. Massey, S. Murphy, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology. EUROCRYPT'91. Proceedings. Springer Verlag*, pp. 17-38, 1991.

[8]. M. Matsui, "Linear cryptanalysis methods for DES cipher", *Advances in Cryptology. EUROCRYPT'93. Proceedings. Springer Verlag*, pp. 386-397, 1994.

[9]. A. Alekseychuk, L. Kovalchuk, E.Skrypnik, A. Shevcov, "Estimates of the practical durability of the block cipher "Kalina" with respect to the methods of difference, linear-cryptanalysis and algebraic attacks based on homomorphisms", *Applied electronics,* vol. 7, no. 3, pp. 203-209, 2008.

[10]. V. Kinzeryavyy, "Top estimates of the stability of block ciphers with randomized nodes replacing the methods of linear and dipferential cryptanalysis", *Information protection*, vol. 15, no. 1, pp. 21–31, 2013.

КРИПТОГРАФИЧЕСКИЙ МЕТОД ЗАЩИТЫ КРИТИЧЕСКИХ АВИАЦИОННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Обеспечение конфиденциальности данных является важным этапом в процессе обеспечения кибербезопасности критических авиационных информационных систем и авиационной отрасли в целом. Известные методы не позволяют в полной мере обеспечить стойкость к кибератакам линейного и дифференциального криптоанализа и необходимую скорость криптографической обработки данных. Учитывая это, в работе разработан криптографический метод защиты критических авиационных информационных систем. На основе данного метода построен блочный симметричный шифр Luna-2k17 и в работе приведена спецификация данного шифра. Также, рассчитано значение верхних оценок параметров, которые характеризуют его практическую стойкость к кибератакам линейного и дифференциального криптоанализа. При одинаковых условиях, проведены экспериментальные исследования по оценки скоростных характеристик шифров, которые показали, что шифр Luna- 2k17 более быстрый за шифр ГОСТ 28147-89 приблизительно в 3,11 раза, а за шифры Калина и AES в 1,271 раза.

Ключевые слова: криптография, блочный шифр, линейный криптоанализ, дифференциальный криптоанализ, защита информации.

CRYPTOGRAPHIC METHOD OF DEFENCE OF CRITICAL AVIATION INFORMATIVE SYSTEMS

Providing of confidentiality of data is the important stage in the process of providing of cyber security of the critical aviation informative systems and aviation industry on the whole. Known methods do not allow to fully provide cyberattacks resistance to linear and differential cryptanalysis and the required speed of cryptographic data processing. Taking into account it, the cryptographic method of defence of the critical aviation information systems is inprocess worked out. On the basis of this method, a block symmetric cipher Luna-2k17 was developed and its specification is given in the work. Also, the values of the upper estimates of parameters that characterize its practical stability to cyber attacks of linear and differential cryptanalysis are calculated. At equal terms, experimental studies are undertaken from the estimation of speed characteristics of ciphers, that showed that cipher Luna-2k17 more faster than a cipher GOST 28147-89 approximately in 3,11 times, than ciphers Kalina and AES in 1,271 times.

Keywords: cryptography, block cipher, linear cryptoanalysis, differential cryptoanalysis, information security.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua.
Гнатюк Сергей Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-Security Academic Department, National Aviation University.

Кінзерявий Василь Миколайович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: v.kinzeryavyy@gmail.com.
Кинзерявый Василий Николаевич, кандидат технических наук, доцент кафедры безопасности информационных технологий, Национальный авиационный университет.
Kinzeryavyy Vasyl, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Ахметов Берик Бахытжанович, кандидат технических наук, доцент, ректор Каспийского государственного университета технологий и инжиниринга им. Ш. Есенова.
E-mail: 1im4best@gmail. com
Ахметов Берік Бахитжанович, кандидат технічних наук, доцент, ректор Каспійського державного університету технологій та інжинірингу ім. Ш. Єсенова.
Akhmetov Berik, PhD in Eng., Associate Professor, rector of Sh. Yessenov Caspian State University oh technologies and engineering.

Кириченко Каріна Сергіївна, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: bezverkhayakarina@gmail.com
Кириченко Карина Сергеевна, аспирант кафедры безопасности информационных технологий, Национальный авиационный университет.
Kyrychenko Karina, Postgraduate of the department of information technology security, National Aviation University.

Ануфрієнко Кирило Петрович, здобувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: akp@nau.edu.ua
Ануфриенко Кирилл Петрович, соискатель кафедры безопасности информационных технологий Национального авиационного университета.
Anufriienko Kyrylo, PhD candidate of Academic Department of IT-security, National Aviation University.