DOI: 10.18372/2410-7840.22.14976
УДК 004.056

СТАНДАРТИЗАЦІЯ СИСТЕМ, КОМПЛЕКСІВ ТА ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ЗАСТОСУВАННЯ У ПОСТ-КВАНТОВОМУ СЕРЕДОВИЩІ

Анна Корченко, Євгенія Іванченко, Наталія Кошкіна, Олександр Кузнецов, Олена Качко, Олександр Потій, Віктор Онопрієнко, Всеволод Бобух

Криптографічий захист інформації (КЗІ) є важливою складовою інформаційної безпеки держави, безпосередньо пов'язаною з подоланням сучасних проблем та викликів в кібернетичному просторі України, нових загроз інформаційній безпеці в критичних інфраструктурах в оборонній та сфері безпеки, промисловості, банківському секторі, економіці тощо. Особливу небезпеку в цьому змісті становлять нові ризики, пов'язані з розробкою та стрімким впровадженням сучасних та перспективних інформаційних технологій, здатних докорінно змінити архітектуру інформаційних систем, існуючі парадигми, сталі принципи побудови та математичні основи сучасних засобів КЗІ. Зокрема, поява та стрімке удосконалення нових обчислювальних засобів, заснованих на принципах та ефектах квантової фізики (т.з. універсальних квантових комп'ютерів) ставить під загрозу саме існування діючих нині та стандартизованих на національному та міжнародному рівнях механізмів (протоколів, алгоритмів та засобів) асиметричної криптографії.

Ключові слова: *квантові обчислювачі, криптографічні алгоритми, інформаційна безпека, інформаційні системи.*

ВСТУП

Найближчим часом через можливість ефективного застосування квантових обчислювачів для вирішення задач криптографічного аналізу, переважна більшість існуючих сьогодні асиметричних механізмів стане вразливою та безпорадною щодо забезпечення навіть найнижчого рівня безпеки, а математичні перетворення, на яких базуються такі криптографічні засоби, відійдуть в історію криптографічної науки. Така перспектива є реальним викликом сьогодення, що змусило національний інститут стандартів і технологій (NIST) США оголосити відкритий конкурс пост-квантових криптографічних перетворень (Post-Quantum Cryptography, PQC), тобто таких, що будуть надійними та безпечними, навіть за умови застосування квантового криптографічного аналізу. Але уже попередній аналіз показує, що навіть у нових міжнародних рішеннях можуть бути закладені вразливості та системні недоліки.

Проєкти, що були подані на конкурс PQC криптографами усього світу, представляють декілька напрямків розвитку пост-квантової криптографії: криптографія на решітках, кодова криптографія, мультиваріативна криптографія, криптографія, що базується на геш-функціях, та симетрична криптографія. При цьому статистика конкурсу демонструє, що найбільше проєктів представлено у контексті перших чотирьох напрямків та згідно з результатами другого туру подібна тенденція зберігається. Таким чином, математичні перетворення, засновані на використанні решіток, завадостійких кодів, багатовимірної криптографії та геш-функцій, потребують поглибленого вивчення та дослідження з метою синтезу криптографічних примітивів, які будуть конкурентоспроможними у контексті перспективних пост-квантових механізмів з урахуванням міжнародних вимог та елементної базі сучасної мікроелектроніки.

За поглядами Агентства Національної Безпеки (NSA) США [1], NIST США [2], Європейського інституту телекомунікаційних стандартів (ETSI) [3] та провідних світових учених [4] повномасштабні універсальні квантові комп'ютери можуть стати доступними для кіберзловмисників у найближчі 10-15 років. Для упередження цих наявних загроз безпеки наприкінці 2016 року NIST США оголосив всесвітній конкурс пост-квантових криптоалгоритмів [5], в якому задіяні найбільш досвідчені та авторитетні наукові установи, зокрема, Інститут квантових обчислень (IQC), Європейський інститут телекомунікаційних стандартів ETSI, міжнародний проект PQCrypto, тощо.

На сьогоднішній день опубліковані (у липні 2020 р.) результати другого раунду конкурсу [6] та оголошено черговий, третій етап. Всі дослідження зосереджено за чотирма напрямками (перетворення на решітках; збиткових кодах; хеш-функціях та мультиваріативні перетворення) та за трьома механізмами (електронний підпис (ЕП); направлене шифрування (НШ) та інкапсуляція ключів (ІК)). Проміжні результати досліджень за другим етапом конкурсу найбільш докладно викладено в [7]. Результати досліджень та порівняльного аналізу кандидатів другого раунду з використанням ПЛІС представлено в [8]. Докладний опис алгоритмів-фіналістів 3-ого раунду наведено в [9]. Окремим напрямком досліджень є симетрична криптографія та побудова квантових криптоалгоритмів, тобто криптографічних перетворень із використанням квантово-механічних властивостей [10].

Всі зазначені напрямки досліджень у безпосередній співпраці із організаторами конкурсу NIST США розробляються та супроводжуються провідними українськими вченими. Зокрема, авторським колективом цієї роботи протягом останніх 5 років було проведено низку пошукових НДР та ДКР з теоретичного обґрунтування та розробки сучасних моделей, методів та механізмів криптографічного перетворення для пост-квантового застосування. Розроблено та впроваджено 4 національні стандарти, зокрема, асиметричного шифрування та інкапсуляції ключів, що відповідає більш жорстким вимогам щодо надійності та безпеки, ніж встановлені NIST США до пост-квантових криптографічних алгоритмів. Закладене теоретичне підґрунтя, виконане моделювання (прототипування) пост-квантових криптографічних систем і технологій, які потребують подальшого продовження досліджень, доповнення та вдосконалення.

МЕТА РОБОТИ

Метою роботи є розробка основних елементів загальнонаціональної системи КЗІ, а саме стандартизація та безпосереднє впровадження в Україні нових моделей, методів та механізмів криптографічного перетворення інформації в умовах можливого застосування квантових засобів криптографічного аналізу, ведення інформаційних та гібридних війн.

ПОСТАНОВКА ЗАДАЧІ

Для досягнення поставленої мети необхідно провести дослідження стану КЗІ стосовно забезпечення інформаційної безпеки держави та механізмів криптографічного перетворення для пост-квантового застосування.

На виконання рішення Уряду України протягом останніх років Державною службою спеціального зв'язку та захисту інформації (Держспецзв'язку) було організовано розробку, дослідження та прийняття трьох нових стандартів симетричного криптографічного перетворення (ДСТУ 7624:2014; ДСТУ 7564:2014; ДСТУ 8845:2019).

Національний стандарт ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування» установлює алгоритм обчислення хеш-значення для послідовностей двійкових символів, що застосовується в криптографічних методах захисту, забезпечення цілісності та автентичності інформації під час її передачі, обробки і зберігання, в тому числі при використанні електронного цифрового підпису, що визначений ДСТУ 4145-2002. Цей стандарт рекомендується використовувати під час розробки засобів криптографічного захисту інформації в інформаційно-телекомунікаційних системах, а також при модернізації діючих систем для заміни функції хешування, що визначена у міждержавному стандарті ГОСТ 34.311-95.

Національний стандарт ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» установлює криптографічний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності (як додаткової послуги) інформації під час її обробки. Стандарт використовується під час розробки засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також при модерні-

зації діючих систем для заміни ДСТУ ГОСТ 28147:2009. Для забезпечення конфіденційності і цілісності послідовностей двійкових символів можливо використання цього стандарту сумісно з ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування», при цьому повинні використовуватись різні ключі шифрування і автентифікації.

Національний стандарт ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення» установлює криптографічний алгоритм симетричного потокового перетворення для забезпечення конфіденційності та цілісності (як додаткової послуги) інформації під час її оброблення. У стандарті описано алгоритм симетричного потокового криптографічного перетворення, який використовує ключовий потік для шифрування відкритого тексту побітовим або поблоковим чином. Ключовий потік генерується лише із секретного ключа та вектора ініціалізації (синхропосилки), отже стандарт визначає синхронний потоковий шифр (за класифікацією з ДСТУ ISO/IEC 18033-4:2015). Стандарт використовують під час розроблення засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також в разі модернізації наявних систем для заміни потокових режимів згідно з ДСТУ ГОСТ 28147:2009. Для забезпечення конфіденційності та цілісності послідовностей двійкових символів можна застосовувати цей стандарт сумісно з ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) та ДСТУ 7564:2014.

Розглянемо основні результати з розробки та дослідження зазначених криптографічних алгоритмів, зосереджуючи увагу на перевагах їх практичного застосування в пост-квантовому середовищі, в умовах ведення інформаційних та гібридних війн.

Національний стандарт ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування». Наприкінці 2014 року до Переліку прийнятих і затверджених національних стандартів України внесено ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування», який був розроблений на замовлення Держспецзв'язку на виконання наказу Мінекономрозвитку від 02 грудня 2014 року № 1431 «Про прийняття національних стандартів України, гармонізованих з європейськими стандартами, міжнародних стандартів як національних стандартів України…» та вводиться в дію 01 квітня 2015 року [11, 12].

Загальні положення. Під функцією гешування H розуміється залежне від вектора ініціалізації $IV \in V_l$, $l \in \{512,1024\}$ відображення повідомлення $M \in V_N$, $N \in \{0,1,..,2^{96}-1\}$ у геш-значення $H(IV,M) \in V_n$, $n \in \{8 \cdot s \mid s = 1,2,...,64\}$, таке що $H^{(IV)} : V_N \to V_n$. Режим роботи функції гешування для $n \in \{8 \cdot s \mid s = 1,2,...,64\}$ позначається «Купина-*n*». Основними режимами роботи функції гешування, що рекомендуються до застосування, є «Купина-256», «Купина-384» і «Купина-512».

Загальна структура перетворення. При формуванні геш-значення повідомлення M завжди доповнюється до довжини, кратної розміру блоку, та поділяється на блоки $m_1, m_2, \ldots, m_k$, кожен з яких має довжину l біт. Вибір l здійснюється відповідно до розміру геш-значення n:

$$l = \begin{cases} 512 \text{ для } 8 \le n \le 256, \\ 1024 \text{ для } 256 < n \le 512, \end{cases}$$

де $n \in \{8 \cdot s \mid s = 1,2,...,64\}$.

Обчислення геш-значення здійснюється за наступною ітеративною процедурою:

$$h_0 = IV,$$

$$h_i = T_l^{\oplus}(h_{i-1} \oplus m_i) \oplus T_l^{+}(m_i) \oplus h_{i-1}, \quad i = 1,2,...,k,$$

$$H(IV,M) = R_{l,n}\left(T_l^{\oplus}(h_k) \oplus h_k\right),$$

де $IV = \begin{cases} 0x4000...00 \text{ для } l = 512, \\ 0x8000...00 \text{ для } l = 1024 \end{cases}$ –

вектор ініціалізації довжиною l біт, $T_l^{\oplus}$, T_l^{+} – бієктивні перетворення, що виконують відображення

вхідного блоку довжиною l біт у вихідний такої ж довжини,

– функція, що повертає n старших біт з вхідного блоку x довжиною l біт ($n<l$). При обробці l-бітових слів представляється у вигляді $R_{l,n}(x)=\left(x>>(l-n)\right)\&\sim\left(0xFF...F<<n\right)$, де результат записується в молодші n біт обчисленого значення.

Структурна схема функції гешування "Купина" наведена на рис. 1.

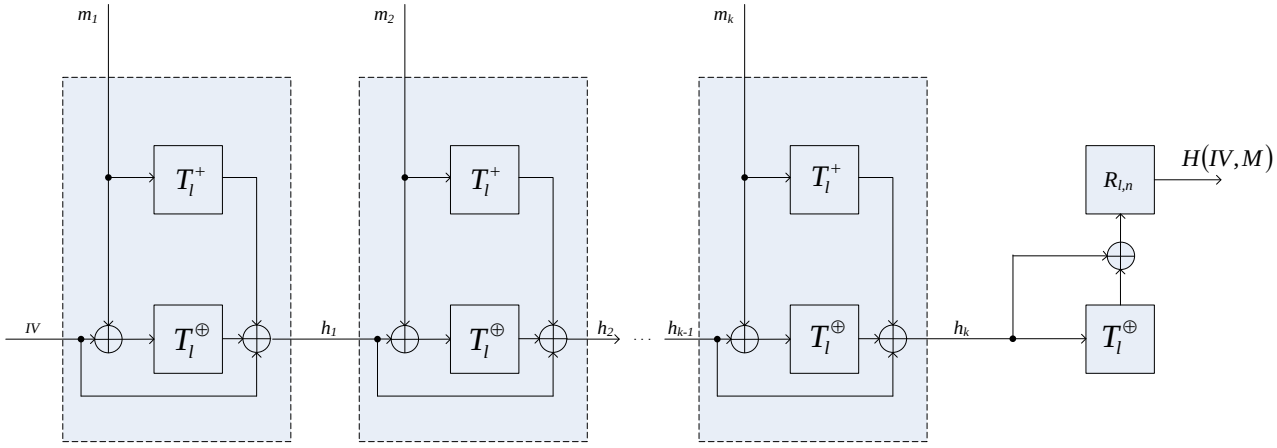

Рис. 1 Структурна схема функції гешування "Купина"

Доповнення повідомлення. На вхід функції гешування подається повідомлення (бітова послідовність) M довжини N, $N\in\left\{0,1,...,2^{96}-1\right\}$, яка задана в бітах. Кожне повідомлення доповнюється, незалежно від його довжини. У кінець повідомлення додається допоміжна інформація, яка містить одиничний біт, необхідну кількість нульових бітів (див. нижче) та довжину повідомлення на вході функції гешування, таким чином, щоб доповнена бітова послідовність мала довжину, кратну розміру внутрішнього стану l, $l\in\{512,1024\}$.

При доповненні спочатку у кінець повідомлення додається одиничний біт «1», потім додаються d нульових бітів, де $d=(-N-97)\bmod l$. Після цього додаються ще 96 біт, в яких записано значення N (найменш значущі байти мають менший номер, тобто використовується формат little endian). Максимальна довжина повідомлення, що може бути оброблено, становить $2^{96}-1$ біт.

Перетворення $T_l^{\oplus}$ та T_l^{+}. Перетворення $T_l^{\oplus}$ та T_l^{+} є бієктивними відображеннями $T_l^{\oplus},T_l^{+}:V_l\to V_l$, $l\in\{512,1024\}$, кожне з яких реалізоване у вигляді ітеративного застосування низки функцій, що обробляють вхідний аргумент $x\in V_l$ як матрицю розміром $8\times c$ байтів, що містить елементи поля GF(2^8). Залежність розміру внутрішнього стану (l), кількості ітерацій (t) та розмірності матриці (c) від розміру геш-значення n наведено у табл. 1.

Таблиця 1

Процес перетворення

Розмір геш-значення	Розмір внутрішнього стану (l)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
$8\le n\le 256$	512	10	8
$256<n\le 512$	1024	14	16

Матриця внутрішнього стану позначається як $G=(g_{i,j})$, $g_{i,j}\in GF(2^8)$. Запис байтів $B_1,B_2,...,B_{l/8}$ перетворень $T_l^{\oplus}$ та T_l^{+} до матриці і зчитування з неї здійснюється по стовпцях (приклад для $l=512$ та $c=8$ див. на рис. 2). $T_l^{\oplus}$ та T_l^{+} визначені наступним чином:

$$T_l^{\oplus}=\prod_{i=0}^{t-1}\left(\psi\circ\tau^{(l)}\circ\pi'\circ\kappa_i^{(l)}\right),\ T_l^{+}=\prod_{i=0}^{t-1}\left(\psi\circ\tau^{(l)}\circ\pi'\circ\eta_i^{(l)}\right),$$

де $\kappa_i^{(l)}$ – функція додавання констант ітерацій за модулем 2, $\eta_i^{(l)}$ – функція додавання констант ітерацій за модулем 2^{64}, π' – шар нелінійного бієктивного відображення, який виконує обробку векторів, заданих на V_8 (байтову підстановку), $\tau^{(l)}$ – перестановка елементів $g_{i,j}\in GF(2^8)$ внутрішнього стану (циклічний зсув при матричному поданні); ψ – лінійне перетворення (множення вектору на матрицю над скінченним полем).

В функціях $\kappa_i^{(l)}$, $\eta_i^{(l)}$, π', $\tau^{(l)}$ і ψ вхідний аргумент $x\in V_l$ та вихідне значення $\chi(x)\in V_l$, $\chi\in\left\{\kappa_i^{(l)},\eta_i^{(l)},\pi',\tau^{(l)},\psi\right\}$ розглядається як матриця розміром $8\times c$ байтів (див. табл.1). Функція $\kappa_i^{(l)}$ здійснює додавання за модулем 2 до кожного стовпця матриці внутрішнього стану $G=(g_{i,j})$ вектора $\omega_{i,j}\in V_{64}$. Для j-го стобця на i-й ітерації перетворення $T_l^{\oplus}$ вектор $\omega_{i,j}=\left((j<<4)\oplus i,0,0,0,0,0,0,0\right)^T$.

Вхідна послідовність							
B_1	B_9	B_{17}	B_{25}	B_{33}	B_{41}	B_{49}	B_{57}
B_2	B_{10}	B_{18}	B_{26}	B_{34}	B_{42}	B_{50}	B_{58}
B_3	B_{11}	B_{19}	B_{27}	B_{35}	B_{43}	B_{51}	B_{59}
B_4	B_{12}	B_{20}	B_{28}	B_{36}	B_{44}	B_{52}	B_{60}
B_5	B_{13}	B_{21}	B_{29}	B_{37}	B_{45}	B_{53}	B_{61}
B_6	B_{14}	B_{22}	B_{30}	B_{38}	B_{46}	B_{54}	B_{62}
B_7	B_{15}	B_{23}	B_{31}	B_{39}	B_{47}	B_{55}	B_{63}
B_8	B_{16}	B_{24}	B_{32}	B_{40}	B_{48}	B_{56}	B_{64}

Внутрішній стан							
$g_{0,0}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,4}$	$g_{0,5}$	$g_{0,6}$	$g_{0,7}$
$g_{1,0}$	$g_{1,1}$	$g_{1,2}$	$g_{1,3}$	$g_{1,4}$	$g_{1,5}$	$g_{1,6}$	$g_{1,7}$
$g_{2,0}$	$g_{2,1}$	$g_{2,2}$	$g_{2,3}$	$g_{2,4}$	$g_{2,5}$	$g_{2,6}$	$g_{2,7}$
$g_{3,0}$	$g_{3,1}$	$g_{3,2}$	$g_{3,3}$	$g_{3,4}$	$g_{3,5}$	$g_{3,6}$	$g_{3,7}$
$g_{4,0}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$	$g_{4,4}$	$g_{4,5}$	$g_{4,6}$	$g_{4,7}$
$g_{5,0}$	$g_{5,1}$	$g_{5,2}$	$g_{5,3}$	$g_{5,4}$	$g_{5,5}$	$g_{5,6}$	$g_{5,7}$
$g_{6,0}$	$g_{6,1}$	$g_{6,2}$	$g_{6,3}$	$g_{6,4}$	$g_{6,5}$	$g_{6,6}$	$g_{6,7}$
$g_{7,0}$	$g_{7,1}$	$g_{7,2}$	$g_{7,3}$	$g_{7,4}$	$g_{7,5}$	$g_{7,6}$	$g_{7,7}$

Рис. 2 Заповнення внутрішнього стану

Функція $\eta_i^{(l)}$ здійснює додавання за модулем 2^{64} до кожного стовпця матриці внутрішнього стану $G=(g_{i,j})$ вектора $\varsigma_{i,j}\in V_{64}$. Для j-го стовпця на i-й ітерації перетворення T_l^{+} вектор $\varsigma_{i,j}$ як

$$\varsigma_{i,j}=(0xF3,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0,\left((c-1-j)<<4\right)\oplus i)^T,$$

де $0xF3$ – молодші 8 біт (при виконанні операції додавання) вектору $\varsigma_{i,j}$.

Функція π' виконує заміну кожного елементу $g_{i,j}$ матриці внутрішнього стану $G=(g_{i,j})$ на $\pi_{i\bmod 4}\left(g_{i,j}\right)$, де $\pi_s:V_8\to V_8, s\in\{0,1,2,3\}$ - підстановки, наведені у додатку А.

Наприклад, нехай $g_{0,0} = 0x22$, тоді $\pi_0(0x22) = 0xA3$.

Функція $\tau^{(l)}$ виконує циклічний зсув вправо рядків матриці стану $G = (g_{i,j})$. Рядки з номерами i=0,1,2, ..,6 матриці зсуваються на i елементів, а рядок з номером 7 зсувається на 7 елементів для $l = 512$ і на 11 елементів для $l = 1024$.

При обчисленні результату функції ψ кожен елемент $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ розглядається як елемент скінченного поля $GF(2^8)$, що утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$, або *0x11d* у шістнадцятковому поданні. Кожен елемент результуючої матриці стану $U = (u_{i,j})$ отримується як результат множення стовпця матриці стану $G = (g_{i,j})$ на вектор над скінченним полем $GF(2^8)$, що утворює циркулянтну матрицю МДР-коду: $u_{i,j} = (v >>> i) \times G_j$, де $v = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$ – вектор, що складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$; G_j – j–й стовпець матриці стану $G = (g_{i,j})$, $G_j=(g_{0j}, g_{1j}\ g_{2j}\ g_{3j}\ g_{4j}\ g_{5j}\ g_{6j}\ g_{7j})^T$.

Алгоритм ДСТУ 7564:2014 є результатом багаторічної плідної співпраці Державної служби спеціального зв'язку та захисту інформації України та провідних українських науковців і враховує досвід та результати проведення міжнародних і відкритого національного конкурсів криптографічних алгоритмів. Криптографічний алгоритм, що визначається ДСТУ 7564:2014, є гнучким, підтримує розмір блока від 128 до 512 бітів, що є унікальним у світі. Підвищена довжина блоку внутрішнього стану унеможливлює ефективне застосування квантових засобів криптографічного аналізу, що робить його придатним для практичного застосування в постквантовому середовищі, в умовах ведення інформаційних та гібридних війн. Практичне впровадження ДСТУ 7564:2014 дозволить суттєво вдосконалити показники ефективності захисту систем, засобів і протоколів криптографічного захисту інформації, що розробляються в Україні, і у деяких випадках зробити їх суттєво кращими ніж наявні та перспективні світові рішення.

Національний стандарт ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення

Цей національний стандарт був розроблений на замовлення Держспецзв'язку та внесений до Переліку прийнятих та затверджених національних стандартів України на виконання наказу Мінекономрозвитку від 29 грудня 2014 року № 1484 «Про прийняття європейських стандартів як національних стандартів України та скасування національних стандартів України» [11, 12].

Стандарт ДСТУ 7624:2014 розроблено задля поступової заміни міждержавного стандарту ДСТУ ГОСТ 28147:2009 (на базі ГОСТ 28147-89, який визначає симетричний блочний алгоритм криптографічного перетворення), а ДСТУ 7564:2014 – для поступової заміни міждержавного стандарту ДСТУ ГОСТ 34.311:2009 (визначає функцію хешування та має посилання на ГОСТ 28147-89), які не відповідають сучасним вимогам до швидкодії і потенційним викликам щодо криптографічної стійкості.

Стандарт ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення" визначає сучасний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності інформації під час її обробки і встановлює режими його роботи (застосування). Криптографічні перетворення, що застосовуються в алгоритмі, відповідають сучасним вимогам щодо рівня криптографічної стійкості та швидкодії.

Алгоритм розроблено з урахуванням існуючих і потенційних загроз, подальшого інтенсивного розвитку інформаційних технологій та необхідності активного використання протягом декількох наступних десятиліть.

Призначення. Під алгоритмом симетричного блокового перетворення $\Im_{l,k}^{(K)}$ у режимі шифрування розуміється пряме і обернене відображення відкритого тексту $M \in V_N$ у шифртекст $C \in V_N$ (і навпаки), що залежить від ключа шифрування $K \in V_k$ і (для деяких режимів) синхропосилки $S \in V_l$: $\Im_{l,k}^{(K)} : V_N \times V_k \to V_N$ або $\Im_{l,k}^{(K)} : V_l \times V_N \times V_k \to V_N$.

Параметри l і k визначають розмір блоку та довжину ключа базового блокового алгоритму.

Під алгоритмом симетричного блокового перетворення $\phi_{l,k}^{(K)}$ у режимі забезпечення цілісності (вироблення імітовставки) розуміється відображення повідомлення $M \in V_N$ в імітовставку (код автентифікації повідомлення), що залежить від ключа автентифікації $K \in V_k$ і (для деяких режимів) синхропосилки $S \in V_l$: $\phi_{l,k}^{(K)}(S,M) \in V_q$, $64 \le q \le l$ таке що $\phi_{l,k}^{(K)} : V_l \times V_N \times V_k \to V_q$.

Криптографічний алгоритм, визначений у цьомустандарті, передбачає можливість одночасного забезпечення конфіденційності та цілісності повідомлення шляхом послідовного застосування відповідних перетворень.

Режими роботи. Криптографічний алгоритм симетричного блокового перетворення використовує базове перетворення як основний елемент при забезпеченні конфіденційності та (або) цілісності. Режими роботи криптографічного алгоритму, визначеного в цьому стандарті, їх позначення та послуги безпеки, які забезпечує відповідний режим, визначені у табл. 2.

Додаткові параметри використання кожного режиму наведені при його описі. Режим роботи криптографічного алгоритму, визначеного у цьому стандарті, позначається наступним чином: „Калина-l/k-позначення режиму-параметри режиму" (для деяких режимів параметри відсутні), де l – розмір блоку базового перетворення, k – довжина ключа.

Наприклад, Калина-256/512-CCM-32,128 визначає використання базового перетворення з розміром блоку 256 бітів, довжиною ключа 512 бітів, застосування у режимі вироблення імітовставки і гамування, довжина конфіденційної (та відкритої) частини повідомлення завжди менша 2^{32} байтів, довжина імітовставки дорівнює 128 бітам. Режим простої заміни збігається з базовим перетворенням, тому крім позначення «Калина-l/k-ECB» може використовуватись позначення «Калина-l/k».

Проста заміна (базове перетворення). Режим простої заміни є компонентом усіх інших режимів роботи криптографічного алгоритму симетричного блокового перетворення. Без додаткових перетворень, визначених іншими режимами, використання простої заміни для захисту повідомлень не рекомендується. Базове перетворення реалізує пряме перетворення (зашифрування) та обернене перетворення (розшифрування).

Таблиця 2

Режими роботи криптографічного алгоритму

№ режиму	Назва режиму	Позначення	Послуга безпеки
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотнім зв'язком за шифртекстом	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифрблоків	CBC	Конфіденційність
6	Гамування зі зворотнім зв'язком за шифргамою	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	цілісність і конфіденційність
9	Індексованої заміни	XTS	конфіденційність
10	Захисту ключових даних	KW	конфіденційність і цілісність

Базове перетворення зашифрування $T_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням $T_{l,k}^{(K)}: V_l \to V_l$, $K \in V_k$, $l,k \in \{128, 256, 512\}$ при цьому $k = l$ або $k = 2 \cdot l$, що реалізоване у вигляді ітеративного застосування низки функцій, які обробляють вхідний аргумент $x \in V_l$ як матрицю внутрішнього стану розміром $8 \times c$ байтів, що містить елементи поля GF(2^8). Базове перетворення розшифрування $U_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням, оберненим до $T_{l,k}^{(K)}$, також реалізованим у вигляді ітеративного перетворення. Залежність кількості ітерацій (t) при реалізації перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$, кількості стовпців матриці внутрішнього стану (c) від розміру блоку (l) і довжини ключа шифрування (k) наведено у табл. 3.

Таблиця 3

Базове перетворення

№ з/п	Розмір блоку (l)	Довжина ключа (k)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

Базове перетворення виконує обробку вхідного блоку даних довжиною l бітів (відкритий текст при зашифруванні або шифртекст при розшифруванні). Матриця внутрішнього стану позначається як $G = (g_{i,j})$, $g_{i,j} \in GF(2^8)$, де $i = \overline{0,7}$, $j = \overline{0,c-1}$.. Запис байтів $B_1, B_2, ..., B_{l/8}$ для перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$ до матриці і зчитування з неї здійснюється по стовпцях.

Приклад запису байтів до внутрішнього стану для $l = 512$ ($k = 512$, $c = 8$) див. на рис. 1.

Базове перетворення зашифрування $T_{l,k}^{(K)}$ визначено наступним чином:

$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \left(\prod_{v=1}^{t-1} \left(\kappa_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi_l' \right) \right) \circ \eta_l^{(K_0)},$$

де l – розмір внутрішнього стану блокового шифру (у бітах);

K – ключ шифрування;

k – довжина ключа шифрування (у бітах) ;

$\eta_l^{(K_v)}$ – функція додавання циклового ключа K_v ($v \in \{0, t\}$) за модулем 2^{64};

π_l' – шар нелінійного бієктивного відображення, який виконує обробку векторів, заданих над V_8 (байтова підстановка);

τ_l – перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вправо при матричному поданні);

ψ_l – лінійне перетворення (множення матриці лінійного перетворення на матрицю внутрішнього стану над скінченним полем);

$\kappa_l^{(K_v)}$ – функція додавання циклового ключа K_v ($v \in \{1,2,...,t-1\}$) за модулем 2 (інволютивне перетворення).

В функціях π_l', τ_l і ψ_l вхідний аргумент $x \in V_l$ та вихідне значення $\chi(x) \in V_l$, $\chi \in \{\pi_l', \tau_l, \psi_l\}$ розглядаються як матриці розміром $8 \times c$ байтів (див. табл. 3). Функції $\eta_l^{(K_v)}$ і $\kappa_l^{(K_v)}$ залежать від параметра $K_v \in V_l$ (циклового ключа v-ї ітерації), мають вхідний аргумент $x \in V_l$ (внутрішній стан шифру), та вихідне значення $\chi(x, K_v) \in V_l$, $\chi \in \{\eta_l^{(K_v)}, \kappa_l^{(K_v)}\}$, при цьому вхідні аргументи та вихідне значення розглядаються як матриці розміром $8 \times c$ байтів.

Функція додавання циклового ключа K_v за модулем 2^{64} $\eta_l^{(K_v)}$ здійснює додавання за модулем 2^{64} стовпців матриці внутрішнього стану $G=(g_{i,j})$ і стовпців матриці циклового ключа $K_v=(k_{i,j}^v)$, при цьому результат також є матрицею розміром $8\times c$ байтів (внутрішнім станом після додавання).

При виконанні додавання менші значущі байти мають менші індекси, тобто використовується формат little endian.

Функція π_l' виконує заміну кожного елементу $g_{i,j}$ матриці внутрішнього стану $G=(g_{i,j})$ на $\pi_{i \bmod 4}(g_{i,j})$, де $\pi_s: V_8 \to V_8, s \in \{0,1,2,3\}$ - підстановки, які наведені у додатку А.

Наприклад, нехай $g_{0,0}=0x23$, тоді $\pi_0(0x23)=0x4F$.

Для здійснення перетворення може використовуватися інший набір підстановок, відмінний від наведеного у додатку А. У цьому випадку набір підстановок має постачатися і застосовуватися в установленому порядку.

Функція τ_l виконує циклічний зсув вправо рядків матриці стану $G=(g_{i,j})$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,..,7\}$, розміру блоку $l \in \{128,256,512\}$, та обчислюється за формулою $\delta_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$. Наприклад, 5-й рядок матриці стану шифра з 256-бітовим блоком зсувається вправо на 2 елемента.

При обчисленні результату функції ψ_l кожен елемент $g_{i,j}$ матриці внутрішнього стану $G=(g_{i,j})$ розглядається як елемент скінченного поля $GF(2^8)$, що утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$, або *0x11d* у шістнадцятковому поданні. Кожен елемент результуючої матриці стану $W=(w_{i,j})$ отримується як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$ за формулою $w_{i,j}=(\upsilon >>> i)\otimes G_j$, де $\upsilon=(0x01,0x01,0x05,0x01,0x08,0x06,0x07,0x04)$ – вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора над скінченним полем; G_j – j–й стовпець матриці стану $G=(g_{i,j})$.

Функція $\kappa_l^{(K_v)}$ має вхідний аргумент $x \in V_l$ (внутрішній стан шифру) і залежить від параметра $K_v \in V_l$ (циклового ключа v-ї ітерації), кожен з яких поданий як матриця розміром $8\times c$ байтів.

Функція $\kappa_l^{(K_v)}$ здійснює побітове додавання (за модулем 2) стовпців матриці внутрішнього стану $G=(g_{i,j})$ і стовпців матриці циклового ключа $K_v=(k_{i,j}^v)$, при цьому результат також є матрицею розміром $8\times c$ байтів (внутрішнім станом після додавання).

Базове перетворення розшифрування $U_{l,k}^{(K)}$ визначено наступним чином:

$$U_{l,k}^{(K)} = {}_{-1}\eta_l^{(K_0)} \circ \left(\prod_{v=t-1}^{1} \left({}_{-1}\pi_l' \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ \kappa_l^{(K_v)} \right) \circ \right.$$

$$\left. {}_{-1}\pi_l' \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ {}_{-1}\eta_l^{(K_t)} \right) \; l,$$

де – розмір внутрішнього стану блокового шифру (у бітах), K – ключ шифрування, k – довжина ключа шифрування (у бітах), ${}_{-1}\eta_l^{(K_v)}$ – функція віднімання циклового ключа K_v ($v \in \{0,t\}$) за модулем 2^{64} (обернена до $\eta_l^{(K_v)}$); ${}_{-1}\psi_l$ – обернене лінійне перетворення (множення матриці оберненого лінійного перетворення на матрицю внутрішнього стану над скінченним полем); ${}_{-1}\tau_l$ – обернена перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вліво при матричному поданні); ${}_{-1}\pi_l'$ – шар оберненого нелінійного бієктивного відображення, який виконує обробку векторів, заданих над V_8 (обернена байтова підстанов-

ка); $\kappa_l^{(K_v)}$ – інволютивна функція додавання циклового ключа K_v ($v \in \{1,2,...,t-1\}$) за модулем 2 (однакова для зашифрування і розшифрування).

Як і при зашифруванні, в функціях ${}_{-1}\pi'$, ${}_{-1}\tau_l$ і ${}_{-1}\psi_l$ вхідний аргумент $x \in V_l$ та вихідне значення $\chi(x) \in V_l$, $\chi \in \{{}_{-1}\pi', {}_{-1}\tau_l, {}_{-1}\psi_l\}$ розглядаються як матриці розміром $8 \times c$ байтів.

Функція ${}_{-1}\eta_l^{(K_v)}$ має два вхідних аргументи $x \in V_l$ (внутрішній стан шифру) і $K_v \in V_l$ (циклový ключ v-ї ітерації) та вихідне значення ${}_{-1}\eta_l^{(K_v)}(x, K_v) \in V_l$, при цьому вхідні аргументи та вихідне значення розглядаються як матриці розміром $8 \times c$ байтів.

Функція віднімання циклового ключа K_v за модулем 2^{64} ${}_{-1}\eta_l^{(K_v)}$ є оберненою до $\eta_l^{(K_v)}$ і здійснює віднімання за модулем 2^{64} стовпців матриці циклового ключа $K_v = (k_{i,j}^v)$ від стовпців матриці внутрішнього стану $G = (g_{i,j})$, при цьому результат також є матрицею розміром $8 \times c$ байтів (внутрішнім станом після віднімання). При виконанні віднімання найменш значущі байти мають менший індекс, тобто використовується формат little endian.

Функція ${}_{-1}\pi_l'$ виконує заміну кожного елементу $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ на ${}_{-1}\pi_{i \bmod 4}(g_{i,j})$, де ${}_{-1}\pi_s : V_8 \to V_8, s \in \{0,1,2,3\}$ - підстановки, які наведені у додатку А. Наприклад, нехай $g_{0,0} = 0xA3$, тоді ${}_{-1}\pi_0(0xA3) = 0x22$. У разі використання підстановок, відмінних від наведених у додатку А, застосовуються відповідні їм обернені.

Функція ${}_{-1}\tau_l$ виконує циклічний зсув вліво рядків матриці стану $G = (g_{i,j})$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,..,7\}$ розміру блоку $l \in \{128,256,512\}$, та обчислюється за формулою $\delta_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$. Наприклад, 4-й рядок матриці стану шифру з 128-бітовим блоком зсувається вліво на 1 елемент.

При обчисленні результату функції ${}_{-1}\psi_l$ кожен елемент $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ розглядається як елемент скінченого поля $GF(2^8)$, що утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$, або *0x11d* у шістнадцятковому поданні.

Кожен елемент результуючої матриці стану ${}_{-1}W = ({}_{-1}w_{i,j})$ отримується як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$ за формулою ${}_{-1}w_{i,j} = ({}_{-1}\upsilon >>> i) \otimes G_j$, де $v = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$ – вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора над скінченним полем; G_j – j–й стовпець матриці $G = (g_{i,j})$.

Гамування. Режим забезпечує конфіденційність повідомлення шляхом шифрування. Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C, $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M. Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметрами режиму є ключ шифрування K, $|K| = k$ та синхропосилка S, $|S| = l$. Додаткові вимоги щодо синхропосилки не накладаються. Режим гамування позначається як Калина-l/k-CTR.

Повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n-1$, $1 \leq |m_n| \leq l$. Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення:

$$c_i = m_i \oplus L_{l,|m_i|}\left(T_{l,k}^{(K)}\left(L_{l,l/2}(s_0+i)\,\|\,R_{l,l/2}(s_0)\right)\right)$$

для $i=1,2,..,n$, $|c_i|=|m_i|$. Результатом зашифрування повідомлення є шифртекст $C=c_1\|c_2\|...\|c_n$.

Шифртекст C ($|C|\geq 1$) подається у вигляді послідовності блоків: $C=c_1\|c_2\|...\|c_n$, $|c_i|=l$ для $i=1,2,..,n-1$, $1\leq|c_n|\leq l$. Початкове значення лічильника s_0 обчислюється як $s_0=T_{l,k}^{(K)}(S)$. Кожен з блоків повідомлення обчислюються відповідно до співвідношення $m_i=c_i\oplus L_{l,|c_i|}(T_{l,k}^{(K)}(L_{l,l/2}(s_0+i)\ \ \|R_{l,l/2})(s_0)))$ для $i=1,2,..,n$.

Результатом розшифрування є повідомлення $M=m_1\|m_2\|...\|m_n$.

Гамування зі зворотнім зв'язком за шифртекстом. Режим забезпечує конфіденційність повідомлення шляхом шифрування. Шифрування виконує пряме відображення повідомлення M ($|M|\geq 1$) у шифртекст C, $|C|=|M|$, та обернене відображення шифртексту C в повідомлення M. Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметрами режиму є ключ шифрування K, $|K|=k$, синхропосилка S, $|S|=l$ та додаткове значення q, яке визначає кількість бітів повідомлення, що обробляються за допомогою одного застосування базового перетворення:

$$q\in\{1,8,64,128,256,512\mid q\leq l\}.$$

Рекомендованим значенням параметра є $q=l$. Додатковою вимогою до синхропосилки в цьому режимі є випадковість, в тому числі непередбачуваність значення, яке буде застосовано для будь-якого повідомлення, до його формування. Режим гамування позначається як Калина-l/k-CFB-q.

Повідомлення M ($|M|\geq 1$) подається у вигляді послідовності блоків: $M=m_1\|m_2\|...\|m_n$, $|m_i|=q$ для $i=1,2,..,n-1$, $1\leq|m_n|\leq q$. Встановлюється значення $c_0^{\#}=T_{l,k}^{(K)}(S)$, $|c_0^{\#}|=l$.

Кожен з блоків шифртекста c_i ($|c_i|=q$) обчислюється відповідно до співвідношення:

$$c_i = m_i \oplus R_{l,|m_i|}\left(c_{i-1}^{\#}\right)$$

для $i=1,2,..,n$ та $c_i^{\#}=T_{l,k}^{(K)}\left(L_{l,l-q}\left(c_{i-1}^{\#}\right)\|\,c_i\right)$ для $i=1,2,..,n-1$, $|c_i^{\#}|=l$. Результатом зашифрування повідомлення є шифртекст $C=c_1\|c_2\|...\|c_n$.

Шифртекст C ($|C|\geq 1$) подається у вигляді послідовності блоків: $C=c_1\|c_2\|...\|c_n$, $|c_i|=q$ для $i=1,2,..,n-1$, $1\leq|c_n|\leq q$. Встановлюються значення $c_0^{\#}=T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i=c_i\oplus R_{l,|c_i|}\left(c_{i-1}^{\#}\right)$ для $i=1,2,..,n$ та $c_i^{\#}=T_{l,k}^{(K)}\left(L_{l,l-q}\left(c_{i-1}^{\#}\right)\|\,c_i\right)$ для $i=1,2,..,n-1$. Результатом розшифрування шифртекста є повідомлення $M=m_1\|m_2\|...\|m_n$.

Вироблення імітовставки. Режим забезпечує цілісність повідомлення шляхом обчислення та перевірки імітовставки.

Режим виконує відображення повідомлення O ($|O|=l\cdot n_o$, де n_o – додатне ціле) в імітовставку h, $|h|\in\{64,128,256,384,512\}$ при $|h|\leq l$, а при перевірці цілісності додатково виконується порівняння обчисленої імітовставки із тією, що була отримана разом із повідомленням. Синхропосилка в цьому режимі не використовується.

Параметрами режиму є ключ автентифікації K, $|K|=k$ та q – довжина імітовставки, $64\leq q\leq l$. Рекомендоване значення є $q=l$.

Режим вироблення імітовставки позначається як Калина-l/k-CMAC-q.

Повідомлення O ($|O|=l\cdot n_o$, де n_o – додатне ціле) подається у вигляді послідовності блоків: $O=o_1\|o_2\|...\|o_{n_o}$, $|o_i|=l$ для $i=1,2,..,n_o$.

Встановлюється значення $c_0=0^l$.

Якщо повідомлення було доповнене, то встановлюється $K_\delta = T_{l,k}^{(K)}(0x00..01)$, де $0x00..01$ – l-бітове подання 1 у форматі little endian; у іншому випадку $K_\delta = T_{l,k}^{(K)}(0^l)$. Для $i = 1,2,..,n_o - 1$ обчислюються $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus o_i)$. Для $i = n_o$ задається $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus o_i \oplus K_\delta)$. Результатом обчислення є імітовставка $h = L_{l,q}(c_{n_o})$.

Для повідомлення M застосовується алгоритм обчислення імітовставки.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із повідомленням, цілісність повідомлення є порушеною.

У іншому випадку цілісність повідомлення підтверджена.

Зчеплення шифрблоків. Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Якщо довжина повідомлення не є кратною розміру блоку базового перетворення, то застосовується алгоритм доповнення. Шифрування виконує пряме відображення повідомлення M ($|M| = l \cdot n$, де n – додатне ціле) у шифртекст C, $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M. Параметрами режиму є ключ шифрування K, $|K| = k$, синхропосилка S, $|S| = l$. Додатковою вимогою до синхропосилки в цьому режимі є випадковість (непередбачуваність значення, яке буде застосовано для будь-якого повідомлення). Режим зчеплення шифр блоків позначається як Калина-l/k-CBC.

Повідомлення M подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n$. Встановлюється значення $c_0 = S$. Для $i = 1,2,..,n$ обчислюються $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus m_i)$. Результатом зашифрування повідомлення є шифртекст $C = c_1 \| c_2 \| ... \| c_n$.

Шифртекст C ($|C| = l \cdot n$, де n – додатне ціле) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n$. Встановлюється значення $c_0 = S$. Для $i = 1,2,..,n$ обчислюються $m_i = c_{i-1} \oplus U_{l,k}^{(K)}(c_i)$. Результатом розшифрування шифртекста є повідомлення $M = m_1 \| m_2 \| ... \| m_n$.

Гамування зі зворотнім зв'язком за шифргамою. Режим забезпечує конфіденційність повідомлення шляхом шифрування. Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C, $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M. Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметрами режиму є ключ шифрування K, $|K| = k$ та синхропосилка S, $|S| = l$.

Додаткові вимоги щодо синхропосилки не накладаються. Режим гамування позначається як Калина-l/k-OFB.

Повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n-1$, $1 \leq |m_n| \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як $\gamma_0 = T_{l,k}^{(K)}(S)$. Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = m_i \oplus L_{l,|m_i|}(\gamma_{i-1})$ для $i = 1,2,..,n$, та $\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1})$ для $i = 1,2,..,n-1$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \| c_2 \| ... \| c_n$. Шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n-1$, $1 \leq |c_n| \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як $\gamma_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i = c_i \oplus L_{l,|m_i|}(\gamma_{i-1})$ для $i = 1,2,..,n$, та $\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1})$ для $i = 1,2,..,n-1$.

Результатом розшифрування шифртекста є повідомлення $M = m_1 \| m_2 \| ... \| m_n$.

Вибіркове гамування із прискореним виробленням імітовставки. Режим забезпечує конфіденційність і цілісність повідомлення шляхом шифрування і обчислення та перевірки імітовставки. Шифрування (гамування) є вибірковим, тобто конфіденційність забезпечується для обраної частини повідомлення (довжина цієї частини обирається в залежності від вимог до засобу криптографічного захисту: від шифрування всього повідомлення до відсутності шифрування взагалі). Повідомлення складається з двох частин: відкритої O (для якої буде забезпечена лише цілісність) та конфіденційної M (для якої буде забезпечена конфіденційність та цілісність), $|O|+|M| \geq 1$. Режим забезпечує цілісність відкритої частини повідомлення O та шифртекста C (зашифрованої частини повідомлення M) шляхом обчислення та перевірки імітовставки.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C, $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M. Крім того, виконується відображення криптограми (відкритої частини повідомлення O і шифртексту) в імітовставку h, $64 \leq |h| \leq l$, а при перевірці цілісності додатково виконується порівняння обчисленої імітовставки із тією, що була отримана разом із повідомленням. Вимоги на кратність довжини повідомлення (відкритої або конфіденційної частини) розміру блоку базового перетворення не накладаються. Параметрами режиму є ключ шифрування K, $|K| = k$, синхропосилка S, $|S| = l$ та q – довжина імітовставки, $64 \leq q \leq l$. Рекомендоване значення $q = l$. Додаткові вимоги щодо синхропосилки не накладаються. Режим вибіркового гамування із прискореним виробленням імітовставки для $|M| \geq 1$ позначається як Калина-l/k-GCM-q (забезпечується конфіденційність та цілісність), для $|M| = 0$ режим позначається як Калина-l/k - GMAC -q (забезпечується тільки цілісність).

Вироблення імітовставки є допоміжним алгоритмом, який використовується при прямому та оберному криптографічному перетворенні для обробки відкритої частини повідомлення O та шифртексту C. Якщо довжина шифртексту C не кратна розміру блоку базового перетворення ($|C| \neq n \cdot l$, $n \in \{0,1,2,...\}$), до нього застосовується алгоритм доповнення: $C^* = c_1^* \| c_2^* \| ... \| c_n^*$, де $|c_i^*| = l$ для $i = 1,2,..,n$. У іншому випадку (доповнення не потрібне) $C^* = C$. Коли довжина відкритої частини повідомлення O не кратна розміру блоку базового перетворення ($|O| \neq n_o \cdot l$, $n_o \in \{0,1,2,...\}$), до неї застосовується алгоритм доповнення, $O^* = o_1^* \| o_2^* \| ... \| o_{n_o}^*$, де $|o_i^*| = l$ для $i = 1,2,..,n_o$. У іншому випадку (доповнення не потрібне) $O^* = O$. Значення параметризованої змінної автентифікації H ($|H| = l$) обчислюється як $H = T_{l,k}^{(K)}(0^l)$. Встановлюються значення $b_0 = 0^l$.

Обчислюються значення $b_i = (o_i^* \oplus b_{i-1}) \bullet_l H$ для $i = 1,2,..,n_o$, $|b_i| = l$. Встановлюється значення $b_0' = b_{n_0}$, $|b_i'| = l$ для $i = 1,2,..,n$. Обчислюються значення $b_i' = (c_i^* \oplus b_{i-1}') \bullet_l H$ для $i = 1,2,..,n$. Встановлюється $B = b_n'$. Довжина відкритої та конфіденційної частини повідомлення (задана у бітах) подається у вигляді бітових послідовностей довжиною $l/2$ бітів кожна (формат little endian): $\lambda_o = |O|$, $\lambda_C = |C|$, $|\lambda_o| = |\lambda_C| = l/2$. Імітовставка h обчислюється як:

$$h = L_{l,q}\left(T_{l,k}^{(K)}\left(B \oplus (\lambda_o \| \lambda_C)\right)\right),$$

а цей пункт визначає пряме перетворення Калина-l/k-GCM-q, коли присутня конфіденційна частина повідомлення M ($|M| \geq 1$).

M подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n-1$, $1 \le |m_n| \le l$. Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$. Кожен з блоків шифртекста обчислюється відповідно до співвідношення:

$$c_i = m_i \oplus L_{l,|m_i|}\left(T_{l,k}^{(K)}\left(L_{l,l/2}(s_0 + i) \| R_{l,l/2}(s_0)\right)\right),$$

для $i = 1,2,..,n$, $|c_i| = |m_i|$. Результатом зашифрування конфіденційної частини повідомлення є шифртекст $C = c_1 \| c_2 \| ... \| c_n$.

Результатом роботи прямого перетворення режиму Калина-l/k-GCM-q є шифртекст C та імітовставка h. Цей пункт визначає обернене перетворення Калина-l/k-GCM-q, коли у складі вхідних даних присутній шифртекст C ($|C| \ge 1$).

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із вхідними даними, цілісність є порушеною. Обробка переривається та повертається повідомлення про порушення цілісності. Якщо цілісність підтверджена, то виконується розшифрування конфіденційної частини повідомлення.

Шифртекст C ($|C| \ge 1$) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n-1$, $1 \le |c_n| \le l$. Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$. Кожен з блоків повідомлення обчислюється відповідно до співвідношення:

$$m_i = c_i \oplus L_{l,|m_i|}\left(T_{l,k}^{(K)}\left(L_{l,l/2}(s_0 + i) \| R_{l,l/2}(s_0)\right)\right),$$

для $i = 1,2,..,n$. Результатом розшифрування шифртекста є повідомлення $M = m_1 \| m_2 \| ... \| m_n$. Результатом роботи оберненого перетворення режиму Калина-l/k-GCM-q є $M = m_1 \| m_2 \| ... \| m_n$ або повідомлення про порушення цілісності. Цей пункт визначає перетворення Калина-l/k- GMAC -q, коли відсутня конфіденційна частина повідомлення M ($|M| = 0$).

Якщо довжина відкритої частини повідомлення O не кратна розміру блоку базового перетворення ($|O| \ne n_o \cdot l$, $n_o \in \{1,2,...\}$), до неї застосовується алгоритм доповнення, $O^* = o_1^* \| o_2^* \| ... \| o_n^*$, де $|o_i^*| = l$ для $i = 1,2,..,n$. У іншому випадку (доповнення не потрібне) $O^* = O$.

Значення параметризованої змінної автентифікації H ($|H| = l$) обчислюється як $H = T_{l,k}^{(K)}(0^l)$. Встановлюється значення $b_0 = 0^l$. Обчислюються значення $b_i = \left(o_i^* \oplus b_{i-1}\right) \bullet_l H$ для $i = 1,2,..,n_o$, $|b_i| = l$. Встановлюється $B = b_{n_o}$, $|B| = l$.

Довжина відкритої та конфіденційної частини повідомлення подається у вигляді бітових послідовностей довжиною $l/2$ бітів кожна (формат little endian): $\lambda_o = |O|$, $\lambda_M = 0^{l/2}$, $|\lambda_o| = |\lambda_M| = l/2$.

Імітовставка h обчислюється як $h = L_{l,q}(T_{l,k}^{(K)}(B \oplus (\lambda_o \| \lambda_M)))$.

Результатом роботи режиму Калина-l/k-GMAC -q є імітовставка h. Цей пункт визначає перетворення Калина-l/k- GMAC -q, коли відсутня конфіденційна частина повідомлення M ($|M| = 0$), а для відкритої частини повідомлення вже обчислена імітовставка.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із повідомленням, цілісність повідомлення є порушеною. У іншому випадку цілісність повідомлення підтверджена.

Вироблення імітовставки і гамування. Режим забезпечує цілісність і конфіденційність повідомлення шляхом вироблення імітовставки та шифрування. Шифрування (гамування) є вибірковим, тобто конфіденційність може забезпечуватися лише для обраної частини повідомлення.

На вхід режиму для прямого перетворення подається повідомлення, що складається з двох частин: відкритої O (для якої буде забезпечена лише цілісність), та конфіденційної M (для якої буде

забезпечена конфіденційність та цілісність), бітова довжина обох частин є кратною 8: $|O| = 8 \cdot r'$, $r' \in \{0,1,2,...\}$ і $|M| = 8 \cdot r$, $r \in \{1,2,...\}$. Режим забезпечує цілісність обох частин повідомлення (O та M) і конфіденційність M.

Для оберненого перетворення на вхід подається відкрита частина O повідомлення та шифртекст, що був сформований при виконанні прямого перетворення.

Параметрами режиму є ключ шифрування K, $|K| = k$, синхропосилка S, $|S| = l$, $N_{\max}$ – найбільша можлива довжина відкритої або конфіденційної частини повідомлення (в бітах), яке повинно бути оброблене засобом криптографічного захисту, та q – довжина імітовставки, яке обирається як $q \in \{64,128,256,384,512 | q \le l\}$.

У якості $N_{\max}$ рекомендується обирати найменше значення, яке задовольняє практичним потребам (наприклад, коли довжина повідомлення завжди менша 4 ГБ, тобто не перевищує $2^{32}-1$ байтів, $N_{\max} = 2^{35}-8$). Мінімальна необхідна кількість байтів $N_Б$ для збереження довжини повідомлення у байтах (тобто $8 \cdot N_Б$ бітів) обчислюється за формулою $N_Б = \left\lfloor \frac{1}{8}(-3 + \log_2 N_{\max}) + 1 \right\rfloor$. Для прикладу $N_{\max} = 2^{35} - 8$ обчислене $N_Б = 4$.

Режим вироблення імітовставки і гамування позначається як Калина-l/k-ССМ-$(8 \cdot N_Б), q$ (наприклад, Калина-256/512-ССМ-32,128 визначає режим ССМ з використанням базового перетворення з розміром блоку 256 бітів, довжиною ключа 512 бітів, довжина конфіденційної частини повідомлення завжди менша 2^{32} байтів і довжина імітовставки дорівнює 128 бітам).

Вироблення імітовставки є допоміжним алгоритмом, який використовується при прямому та оберненому криптографічному перетворенні для обробки відкритої частини повідомлення O та конфіденційної частини M. Формується заголовок автентифікації G_1, $|G_1| = l$, який складається із молодших байтів синхропосилки, до яких додане поле довжиною $N_Б$ байтів, що містить запис довжини конфіденційної частини повідомлення у форматі little endian, та байт прапорців таким чином, щоб загальний розмір заголовку дорівнював розміру блоку базового перетворення.

Якщо наявна відкрита частина повідомлення ($|O| > 0$), то довжина цієї частини подається у вигляді бітової послідовності довжиною $8 \cdot N_Б$ бітів (формат little endian): $\lambda_o = |O|/8$, $|\lambda_o| = 8 \cdot N_Б$. Формується блок довжини відкритої частини повідомлення G_2 шляхом додавання $(l - (|O| \bmod l) - 8 \cdot N_Б) \bmod l$ нульових бітів до довжини відкритої частини: $G_2 = (\lambda_o \| 0^{(l-(|O| \bmod l)-8 \cdot N_Б) \bmod l})$ таким чином, щоб довжина послідовності $(G_1 \| G_2 \| O)$ була кратною довжині блоку базового перетворення. Послідовність $(G_1 \| G_2 \| O)$ подається у вигляді блоків $(G_1 \| G_2 \| O) = (g_1 \| g_2 \|, g_3 \| ... \| g_{n_g})$ де $n_g = |(G_1 \| G_2 \| O)| / l$.

Встановлюється значення $b_0 = 0^l$. Для $i = 1,2,..,n_g$ обчислюються $b_i = T_{l,k}^{(K)}(b_{i-1} \oplus g_i)$, $|b_i| = l$. Встановлюється $B = b_{n_g}$, $|B| = l$.

Якщо відкрита частина повідомлення відсутня ($|O| = 0$), то встановлюється $B = G_1$, $|B| = l$. У разі, коли довжина конфіденційної частини повідомлення M не є кратною розміру блоку базового перетворення, то застосовується алгоритм доповнення для формування доповненої конфіденційної частини $M^* = m_1^* \| m_2^* \| ... \| m_n^*$, де $|m_i^*| = l$ для $i = 1,2,..,n$. Встановлюється значення $b_0' = B$, $|b_0'| = l$. Для $i = 1,2,..,n$ обчислюються $b_i' = T_{l,k}^{(K)}(b_{i-1}' \oplus m_i^*)$, $|b_i| = l$. Імітовставка h обчислюється як $h = L_{l,q}(b_n')$. Для відкритої частини повідомлення O та конфіденційної частини повідомлення M обчислюється

імітовставка h. Повідомлення для зашифрування M'' складається з конфіденційної частини повідомлення (M) та імітовставки h:

$$M'' = M \| h, \quad M'' = m_1'' \| m_2'' \| ... \| m_{n_m}'', \quad |m_i''| = l$$

для $i = 1,2,..,n_m - 1$, $1 \le |m_{n_m}''| \le l$.

Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = m_i'' \oplus L_{l,|m_i''|}\left(T_{l,k}^{(K)}\left(L_{l,l/2}(s_0 + i) \| R_{l,l/2}(s_0)\right)\right)$ для $i = 1,2,..,n_m$, $|c_i| = |m_i''|$. Результатом роботи режиму є шифртекст:

$$C = c_1 \| c_2 \| ... \| c_n.$$

При розшифруванні шифртекст C ($|C| \ge 1$) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n-1$, $1 \le |c_n| \le l$. Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків отриманої бітової послідовності обчислюється відповідно до співвідношення $m_i'' = c_i \oplus L_{l,|m_i|}\left(T_{l,k}^{(K)}\left(L_{l,l/2}(s_0 + i) \| R_{l,l/2}(s_0)\right)\right)$ для $i = 1,2,..,n$.

Результатом розшифрування шифртекста є $M'' = m_1'' \| m_2'' \| ... \| m_{n_m}''$, $|m_i''| = l$ для $i = 1,2,..,n_m - 1$, $1 \le |m_{n_m}''| \le l$.

З M'' отримується імітовставка $h' = R_{|M''|,q}(M'')$ та конфіденційна частина повідомлення $M = L_{|M''|,|M''|-q}(M'')$. Для відкритої частини повідомлення O та розшифрованої конфіденційної частини повідомлення M обчислюється імітовставка h.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із повідомленням ($h \ne h'$), обробка переривається та повертається повідомлення про порушення цілісності.

У іншому випадку цілісність повідомлення підтверджена, і результатом роботи режиму є конфіденційна частина повідомлення M.

Індексована заміна. Режим забезпечує конфіденційність повідомлення шляхом шифрування. Це перетворення не забезпечує криптографічну послугу збереження цілісності повідомлення, але у випадку модифікації будь-якого блоку шифртексту відповідний блок відкритого тексту після розшифрування буде мати псевдовипадкове значення (його зміст буде цілком зіпсований), а інші блоки залишаться непошкодженими. Шифрування виконує пряме відображення повідомлення M ($|M| \ge l$) у шифртекст C, $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M. Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K, $|K| = k$ та синхропосилка S, $|S| = l$.

Додаткові вимоги щодо синхропосилки не накладаються. У разі, коли розмір повідомлення є кратним розміру блоку базового перетворення, виконується шифрування без доповнення.

У іншому випадку застосовується модифікований алгоритм із доповненням. Режим індексованої заміни позначається як Калина-l/k-XTS (без доповнення) або Калина-l/k-XTS-p (із доповненням).

Повідомлення M ($|M| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n$. Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$. Кожен з блоків шифртекста обчислюється відповідно до співвідношення:

$$c_i = \left(T_{l,k}^{(K)}\left(m_i \oplus \left(\alpha_l^i \bullet_l s_0\right)\right)\right) \oplus \left(\alpha_l^i \bullet_l s_0\right)$$

для $i = 1,2,..,n$, $|c_i| = |m_i|$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \| c_2 \| ... \| c_n$.

Шифртекст C ($|C| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n$.

Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$. Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i = \left(U_{l,k}^{(K)}\left(c_i \oplus \left(\alpha_l^i \bullet_l s_0\right)\right)\right) \oplus \left(\alpha_l^i \bullet_l s_0\right)$ для $i = 1,2,..,n$. Результатом розшифрування є повідомлення $M = m_1 \| m_2 \| ... \| m_n$.

Повідомлення M ($|M| > l$) подається у вигляді послідовності блоків: $M = m_1 \| m_2 \| ... \| m_n$, $|m_i| = l$ для $i = 1,2,..,n-1$, $1 \le |m_n| < l$. Блоки $m_1, m_2, ..., m_{n-1}$ обробляються для отримання фрагменту шифртексту $C^* = c_1 \| c_2 \| ... \| c_{n-2} \| c_{n-1}$.

Обчислюється:

$$c_n = \left(T_{l,k}^{(K)}\left(\left(m_n \| R_{l,l-|m_n|}(c_{n-1})\right) \oplus \left(\alpha_l^n \bullet_l s_0\right)\right)\right) \oplus \left(\alpha_l^n \bullet_l s_0\right),$$

де $s_0 = T_{l,k}^{(K)}(S)$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \| c_2 \| ... \| c_{n-2} \| c_n \| L_{l,|m_n|}(c_{n-1})$.

Шифртекст C ($|C| > l$) подається у вигляді послідовності блоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l$ для $i = 1,2,..,n-1$, $1 \le |c_n| < l$. Блоки $c_1, c_2, ..., c_{n-2}$ обробляються для отримання фрагменту відкритого тексту $M^* = m_1 \| m_2 \| ... \| m_{n-2}$.

Обчислюються $m_n^* = \left(U_{l,k}^{(K)}\left(c_{n-1} \oplus \left(\alpha_l^n \bullet_l s_0\right)\right)\right) \oplus \left(\alpha_l^n \bullet_l s_0\right)$, де $s_0 = T_{l,k}^{(K)}(S)$.

Результатом розшифрування є повідомлення $M = m_1 \| m_2 \| ... \| m_{n-1} \| L_{l,|c_n|}(m_n^*)$.

Захист ключових даних. Режим забезпечує конфіденційність та цілісність повідомлення. Шифрування виконує пряме відображення повідомлення M ($|M| \ge l$) у шифртекст C, $|M| < |C| < |M| + 2 \cdot l$, та обернене відображення шифртексту C в повідомлення M. Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметром режиму є ключ шифрування K, $|K| = k$. У разі, коли розмір повідомлення є кратним розміру блоку базового перетворення, виконується шифрування без доповнення.

У іншому випадку застосовується алгоритм із доповненням. Режим захисту ключових даних позначається як Калина-l/k-KW (без доповнення) або Калина-l/k - KW-p (із доповненням). До повідомлення M ($|M| = l \cdot r$, де r – додатне ціле) додається 0^l для отримання M^*: $M^* = M \| 0^l$. M^* подається у вигляді послідовності напівблоків: $M^* = m_1^* \| m_2^* \| ... \| m_n^*$, $|m_i^*| = l/2$ для $i = 1,2,..,n$ та $n = 2 \cdot (r+1)$. Встановлюється $V = (n-1) \cdot 6$ і $B^0 = m_1^*$, де $|B^j| = l/2$ для $j = 0,1,...,V$.

Задається $b_i^0 = m_i^*$ для $i = 2,..,n$, де $|b_i^j| = l/2$ для $j = 0,1,...,V$.

Для $j = 1,...,V$ обчислюється $B^j = R_{l,l/2}(T_{l,k}^{(K)}(B^{j-1} \| b_2^{j-1})) \oplus \mu_{l/2}^{(j)}$, $b_n^j = L_{l,l/2}(T_{l,k}^{(K)}(B^{j-1} \| b_2^{j-1}))$ та $b_i^j = b_{i+1}^{j-1}$ для $i = 2,..,n-1$. Задається $c_1 = B^V$ і $c_i = b_i^V$ для $i = 2,..,n$. Результатом є шифртекст $C = c_1 \| c_2 \| ... \| c_n$.

Шифртекст C ($|C| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності напівблоків: $C = c_1 \| c_2 \| ... \| c_n$, $|c_i| = l/2$ для $i = 1,2,..,n$ та $n = 2 \cdot r$. Встановлюється $V = (n-1) \cdot 6$ і $B^V = c_1$, де $|B^j| = l/2$ для $j = 0,1,...,V$. Задається $b_i^V = c_i$ для $i = 2,..,n$, де $|b_i^j| = l/2$ для $j = 0,1,...,V$.

Для $j = V, V-1, ..., 1$ обчислюється $B^{j-1} = L_{l,l/2}(U_{l,k}^{(K)}(b_n^j \| (B^j \oplus \mu_{l/2}^{(j)})))$, $b_2^{j-1} = R_{l,l/2}\left(U_{l,k}^{(K)}\left(b_n^j \| \left(B^j \oplus \mu_{l/2}^{(j)}\right)\right)\right)$ і $b_{i+1}^{j-1} = b_i^j$ для $i = 2,..,n-1$. Задається $m_1^* = B^0$ і $m_i^* = b_i^0$ для $i = 2,..,n$. Формується $M^* = m_1^* \| m_2^* \| ... \| m_n^*$. У разі, коли $R_{n \cdot l/2,l}(M^*)$ не дорівнює 0^l,

повертається повідомлення про порушення цілісності. У іншому випадку повертається розшифроване повідомлення $M = L_{n\cdot l/2,n\cdot l/2-l}\left(M^*\right)$. До повідомлення M ($|M|>l$) додається бітове подання довжини $\mu_{l/2}^{(|M|)}$, після чого до результату $\left(M \,\|\, \mu_{l/2}^{(|M|)}\right)$ застосовується алгоритм доповнення для отримання доповненого повідомлення $M'' = m_1'' \| m_2'' \| \ \ ... \| m_{n_m}''$, $|m_i''| = l$ для $i = 1,2,..,n_m$. Доповнене повідомлення M'' обробляється для отримання шифртексту $C = c_1 \| c_2 \| ... | c_{n_m}$, який є результатом роботи режиму. Шифртекст C ($|C| = l\cdot r$, де r – додатне ціле) обробляються для отримання доповненого повідомлення M''. Якщо результатом роботи є повідомлення про порушення цілісності, подальша обробка припиняється із повертанням повідомлення про порушення цілісності. У іншому випадку до доповненого повідомлення M'' застосовується алгоритм зняття доповнення повідомлення. Якщо результатом є помилка оберненого перетворення, подальша обробка припиняється із повідомленням про порушення цілісності. У разі, коли $\mu_{l/2}^{(|M''|-l/2)} \neq R_{|M''|,l/2}(M'')$, повертається повідомлення про порушення цілісності.

При $\mu_{l/2}^{(|M''|-l/2)} = R_{|M''|,l/2}(M'')$ результатом роботи режиму є відкритий текст:

$$M = L_{|M''|,|M''|-l/2}(M'').$$

Таким чином, ДСТУ 7624:2014 визначає десять різних режимів роботи (застосування), які широко поширені відповідно до міжнародного стандарту ISO/IEC 10116:2006.

Це спрямовано на забезпечення широкої застосовності ДСТУ 7624:2014, у тому числі для захисту інформації, що передається комп'ютерними мережами (Інтернет), прозорого шифрування жорстких дисків та знімних носіїв, електронних документів, ключових даних тощо. Наявність такої кількості режимів роботи надає можливість ефективної реалізації систем, засобів і протоколів криптографічного захисту інформації в інформаційно-телекомунікаційних системах різноманітного призначення.

Криптографічний алгоритм блокового шифрування, що визначається ДСТУ 7624:2014, є гнучким, підтримує розмір блока та довжину ключа від 128 до 512 бітів.

Порівняно з відомим міжнародним стандартом AES (ISO/IEC 18033-3:2010), алгоритм ДСТУ 7624:2014 забезпечує вищий рівень криптографічної стійкості (із можливістю застосування блока та ключа шифрування включно до 512 бітів) і аналогічну або вищу швидкодію на сучасних і перспективних програмних і програмно-апаратних платформах.

Підвищена довжина внутрішнього стану унеможливлює ефективне застосування квантових засобів криптографічного аналізу, що робить цей алгоритм найбільш придатним для практичного застосування в пост-квантовому середовищі, в умовах ведення інформаційних та гібридних війн.

Національний стандарт ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення»

Потоковий симетричний шифр, що описаний у національному стандарті України ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації.

Алгоритм симетричного потокового перетворення», визначає алгоритм генерації ключового потоку «СТРУМОК» (англ. STRUMOK), відповідний стандарт набрав чинності з 1 жовтня 2019 року наказом ДП «УкрНДНЦ» від 2 квітня 2019 року № 85 [14, 15].

Основними структурними компонентами генератору ключових потоків *СТРУМОК* є регістр зсуву з лінійним зворотнім зв'язком (*РЗЛЗЗ*) та скінченний автомат (*СА*), в якому виконується нелінійне перетворення.

Криптоалгоритм орієнтований на 64-розрядні обчислювальні системи, отже розмір слова визначено рівним 64 бітам.

Для запису байтів використовується подання

від старшого до молодшого. Вхідні дані використовуються для ініціалізації змінної стану $S_i (i \geq 0)$, яка складається з вісімнадцяти 64-бітових блоків, до складу яких входить дві компоненти: 16 змінних $s^{(i)}$ – комірок регістра зсуву з лінійним зворотнім зв'язком: $s^{(i)} = (s_{15}^{(i)}, s_{14}^{(i)}, \ ..., s_0^{(i)})$; два регістри скінченного автомату $r^{(i)}$: $r^{(i)} = (r_2^{(i)}, r_1^{(i)})$. На виході отримуємо ключовий потік (гаму шифру), який формується з 64-бітових слів Z_i. Схематичне зображення генератору ключових потоків *СТРУМОК* у режимі генерації гами шифру наведено на рисунку 3.

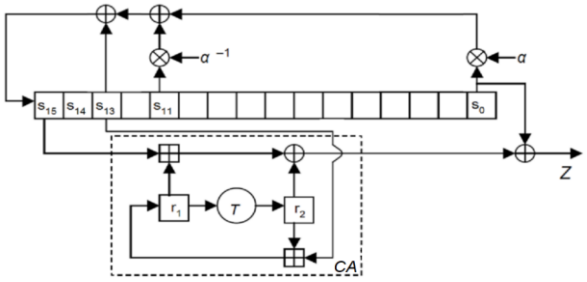

Рис. 3 Схематичне зображення генератору ключових потоків *СТРУМОК* у режимі генерації гами шифру

В свою чергу поле $GF(2^8)$ будується за примітивним над полем $GF(2)$ поліномом $p(y) = y^8 + y^4 + y^3 + y^2 + 1$, а коефіцієнти поліному $g(z)$ подаються через ступінь примітивного елементу β поля $GF(2^8)$, тобто β – корінь поліному $p(y)$.

Таким чином, маємо вежу полів: $GF(2) \subset GF(2^8) \subset GF(2^{64}) \subset GF(2^{1024})$, де: поле $GF(2^{1024})$ задається відводами зворотного зв'язку *РЗЛЗЗ* як факторкільце $GF(2^{64})[x]/(f(x))$, поле $GF(2^{64})$ задається як факторкільце $GF(2^8)[z]/(g(z))$, поле $GF(2^8)$ задається як факторкільце $GF(2)[y]/(p(y))$. Отже період вихідної послідовності *РЗЛЗЗ* є максимальним і дорівнює $2^{1024} - 1$.

Структурно в алгоритмі *СТРУМОК* можна виділити три основні функції: функція ініціалізації *Init*, яка приймає в якості вхідних даних ключ *K* (256 біт або 512 біта) і вектор ініціалізації *IV* (256 біт), і виробляє початкове значення змінної стану $S_0 = (s^{(0)}, r^{(0)})$; функція наступного стану *Next*, яка приймає на вхід змінну стану $S_i = (s^{(i)}, r^{(i)})$ і виробляє наступне значення змінної стану $S_{i+1} = (s^{(i+1)}, r^{(i+1)})$.

Функція *Next* може виконуватися в двох режимах, в залежності від способу виконання ітерації – як частини реалізації або як частини нормального режиму генерації вихідних даних; функція ключового потоку *Strm*, що приймає на вході змінну стану $S_i = (s^{(i)}, r^{(i)})$ і виробляє на виході 64-бітний ключовий потік Z_i.

Функція ініціалізації внутрішнього стану *Init* описується наступним чином.

Вхід: 256 або 512-бітний ключ *K*, 256-бітний вектор ініціалізації *IV*.

Вихід: початкове значення змінної стану $S_0 = (s^{(0)}, r^{(0)})$.

Ключ для режиму *СТРУМОК-256* можна представити у вигляді чотирьох 64-бітних слів $K = (K_3, K_2, K_1, K_0)$, а для 512-бітного ключа – у вигляді восьми 64-бітних слів $K = (K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0)$ де K_3 та K_7, відповідно для 256 и 512 біт, найбільш значущі слова, а K_0 – найменш значущі. Вектор ініціалізації можна представити у вигляді чотирьох 64-бітних слів $IV = (IV_3, IV_2, IV_1, IV_0)$ де IV_3 – найбільш значуще слово, а IV_0 – найменш значуще.

1. В 16 комірок РЗЛЗЗ заноситься значення ключа.

Для версії з 256-бітним ключем виконуються операції:

$s_{15}^{(-33)} = \neg K_0$, $s_{14}^{(-33)} = K_1$, $s_{13}^{(-33)} = \neg K_2$, $s_{12}^{(-33)} = K_3$, $s_{11}^{(-33)} = K_0$, $s_{10}^{(-33)} = \neg K_1$, $s_9^{(-33)} = K_2$, $s_8^{(-33)} = K_3$, $s_7^{(-33)} = \neg K_0$, $s_6^{(-33)} = \neg K_1$, $s_5^{(-33)} = K_2 \oplus IV_3$, $s_4^{(-33)} = K_3$, $s_3^{(-33)} = K_0 \oplus IV_2$, $s_2^{(-33)} = K_1 \oplus IV_1$, $s_1^{(-33)} = K_2$, $s_0^{(-33)} = K_3 \oplus IV_0$.

Для версії з 512-бітним ключем *K* виконуються операції:

$s_{15}^{(-33)} = K_0$, $s_{14}^{(-33)} = \neg K_1$, $s_{13}^{(-33)} = K_2$, $s_{12}^{(-33)} = K_3$, $s_{11}^{(-33)} = \neg K_7$, $s_{10}^{(-33)} = K_5$, $s_9^{(-33)} = \neg K_6$, $s_8^{(-33)} = K_4 \oplus IV_3$, $s_7^{(-33)} = \neg K_0$, $s_6^{(-33)} = K_1$, $s_5^{(-33)} = K_2 \oplus IV_2$,

$s_4^{(-33)} = K_3$, $s_3^{(-33)} = K_4 \oplus IV_1$, $s_2^{(-33)} = K_5$, $s_1^{(-33)} = K_6$, $s_0^{(-33)} = K_7 \oplus IV_0$.

2. Виконується 32 ініціюючих такти без генерації ключового потоку, тобто 4 повних циклів. Формально це подається наступним чином:

$S_{-1} = Next^{32}(S_{-33}, INIT)$, що означає 32 ітерації з виконання функції *Next* у режимі ініціалізації *INIT*, $S_{-33} = (s^{(-33)}, r^{(-33)})$ –значення змінної стану: обраховані на попередньому кроці 16 комірок регістра зсуву $s^{(-33)}$ та початкові нульові значення двох регістрів $r^{(-33)} = (r_2^{(-33)}, r_1^{(-33)})$ скінченного автомату, що у шістнадцятковому поданні мають вигляд $r^{(-33)} = (0000000000000000, 0000000000000000)$.

3. Розраховується початкове значення змінної стану $S_0 = (s^{(0)}, r^{(0)})$ за правилом:

$S_0 = Next(S_{-1})$, тобто шляхом виконання функції *Next* у звичайному режимі.

4. Виводиться вихідне значення $S_0 = (s^{(0)}, r^{(0)})$.

Функція наступного стану *Next* описується наступним чином.

Вхід: Змінна стану $S_i = (s^{(i)}, r^{(i)})$, обраний режим (звичайний, або режим ініціалізації). За замовчуванням використовується звичайний режим.

Вихід: Наступне значення змінної стану $S_{i+1} = (s^{(i+1)}, r^{(i+1)})$.

1. Виконується нелінійна підстановка для оновлення значення регістру $r_2^{(i+1)}$ скінченного автомату. Для цього розраховується значення функції T: $r_2^{(i+1)} = T(r_1^{(i)})$.

2. Оновлюється значення регістру $r_1^{(i+1)}$ скінченного автомату. Для цього розраховується значення: $r_1^{(i+1)} = r_2^{(i)} +_{64} s_{13}^{(i)}$, де $+_{64}$ позначає операцію додавання цілих чисел за модулем 2^{64} (у схемі на рисунках 1 та 2 цю операцію позначено як ⊞).

3. Оновлюється значення 15 комірок *РЗЛЗЗ* $s_j^{(i+1)} = s_{j+1}^{(i)}$ для всіх $j = 0, 1, \ldots, 14$.

4. Оновлюється значення 16-ї комірки *РЗЛЗЗ*. Якщо встановлено звичайний режим функції *Next* значення цієї комірки обчислюється за правилом:

$$s_{15}^{(i+1)} = (s_0^{(i)} \otimes \alpha) \oplus (s_{11}^{(i)} \otimes \alpha^{-1}) \oplus s_{13}^{(i)}.$$

Якщо встановлено режим ініціалізації функції *Next* значення обчислюється за правилом:

$$s_{15}^{(i+1)} = FSM(s_{15}^{(i)}, r_1^{(i)}, r_2^{(i)}) \oplus (s_0^{(i)} \otimes \alpha) \oplus (s_{11}^{(i)} \otimes \alpha^{-1}) \oplus s_{13}^{(i)}.$$

Операції множення $\otimes$ на α та на α^{-1}, а також сутність функції *СА* пояснюються далі.

5. Обчислюється та виводиться значення змінної стану $S_i = (s^{(i)}, r^{(i)})$.

Функція ключового потоку *Strm* описується таким чином.

Вхід: Змінна стану $S_i = (s^{(i)}, r^{(i)})$.

Вихід: 64-бітовий ключовий потік Z_i.

1. Обчислюється значення

$$Z_i = FSM(s_{15}^{(i)}, r_1^{(i)}, r_2^{(i)}) \oplus s_0^{(i)}.$$

2. Виводиться вихідне значення Z_i.

Функція скінченного автомату позначається як $FSM(x, y, z)$ та описується наступним чином.

Вхід: три 64-бітових рядка x, y і z.

Вихід: 64-бітовий рядок *q*.

1. Обчислюється значення $q = (x +_{64} y) \oplus z$.

2. Виводиться вихідне значення *q*.

Функція нелінійної підстановки *T* реалізує перестановку елементів скінченного поля $GF(2^{64})$ за допомогою компонентів національного стандарту блокового симетричного криптоперетворення ДСТУ 7624:2014.

Вхід: 64-бітовий рядок *w*.

Вихід: 64-бітовий рядок $T = T(w)$.

1. Вхідний 64-бітовий рядок *w* розбивається на підблоки w_j по 8 біт:

$$w = (w_7, w_6, w_5, w_4, w_3, w_2, w_1, w_0),$$

2. Для кожного підблоку w_j виконується підстановка з алгоритму ДСТУ 7624:2014 за допомогою чотирьох табличних перетворень $\pi_0, \pi_1, \pi_2, \pi_3$.

Підстановка π_0:

A8 43 5F 06 6B 75 6C 59 71 DF 87 95 17 F0 D8 09
6D F3 1D CB C9 4D 2C AF 79 E0 97 FD 6F 4B 45 39
3E DD A3 4F B4 B6 9A 0E 1F BF 15 E1 49 D2 93 C6
92 72 9E 61 D1 63 FA EE F4 19 D5 AD 58 A4 BB A1
DC F2 83 37 42 E4 7A 32 9C CC AB 4A 8F 6E 04 27
2E E7 E2 5A 96 16 23 2B C2 65 66 0F BC A9 47 41
34 48 FC B7 6A 88 A5 53 86 F9 5B DB 38 7B C3 1E
22 33 24 28 36 C7 B2 3B 8E 77 BA F5 14 9F 08 55
9B 4C FE 60 5C DA 18 46 CD 7D 21 B0 3F 1B 89 FF
EB 84 69 3A 9D D7 D3 70 67 40 B5 DE 5D 30 91 B1
78 11 01 E5 00 68 98 A0 C5 02 A6 74 2D 0B A2 76
B3 BE CE BD AE E9 8A 31 1C EC F1 99 94 AA F6 26
2F EF E8 8C 35 03 D4 7F FB 05 C1 5E 90 20 3D 82
F7 EA 0A 0D 7E F8 50 1A C4 07 57 B8 3C 62 E3 C8
AC 52 64 10 D0 D9 13 0C 12 29 51 B9 CF D6 73 8D
81 54 C0 ED 4E 44 A7 2A 85 25 E6 CA 7C 8B 56 80

Підстановка π_1:

CE BB EB 92 EA CB 13 C1 E9 3A D6 B2 D2 90 17 F8
42 15 56 B4 65 1C 88 43 C5 5C 36 BA F5 57 67 8D
31 F6 64 58 9E F4 22 AA 75 0F 02 B1 DF 6D 73 4D
7C 26 2E F7 08 5D 44 3E 9F 14 C8 AE 54 10 D8 BC
1A 6B 69 F3 BD 33 AB FA D1 9B 68 4E 16 95 91 EE
4C 63 8E 5B CC 3C 19 A1 81 49 7B D9 6F 37 60 CA
E7 2B 48 FD 96 45 FC 41 12 0D 79 E5 89 8C E3 20
30 DC B7 6C 4A B5 3F 97 D4 62 2D 06 A4 A5 83 5F
2A DA C9 00 7E A2 55 BF 11 D5 9C CF 0E 0A 3D 51
7D 93 1B FE C4 47 09 86 0B 8F 9D 6A 07 B9 B0 98
18 32 71 4B EF 3B 70 A0 E4 40 FF C3 A9 E6 78 F9
8B 46 80 1E 38 E1 B8 A8 E0 0C 23 76 1D 25 24 05
F1 6E 94 28 9A 84 E8 A3 4F 77 D3 85 E2 52 F2 82
50 7A 2F 74 53 B3 61 AF 39 35 DE CD 1F 99 AC AD
72 2C DD D0 87 BE 5E A6 EC 04 C6 03 34 FB DB 59
B6 C2 01 F0 5A ED A7 66 21 7F 8A 27 C7 C0 29 D7

Підстановка π_2:

93 D9 9A B5 98 22 45 FC BA 6A DF 02 9F DC 51 59
4A 17 2B C2 94 F4 BB A3 62 E4 71 D4 CD 70 16 E1
49 3C C0 D8 5C 9B AD 85 53 A1 7A C8 2D E0 D1 72
A6 2C C4 E3 76 78 B7 B4 09 3B 0E 41 4C DE B2 90
25 A5 D7 03 11 00 C3 2E 92 EF 4E 12 9D 7D CB 35
10 D5 4F 9E 4D A9 55 C6 D0 7B 18 97 D3 36 E6 48
56 81 8F 77 CC 9C B9 E2 AC B8 2F 15 A4 7C DA 38
1E 0B 05 D6 14 6E 6C 7E 66 FD B1 E5 60 AF 5E 33
87 C9 F0 5D 6D 3F 88 8D C7 F7 1D E9 EC ED 80 29
27 CF 99 A8 50 0F 37 24 28 30 95 D2 3E 5B 40 83
B3 69 57 1F 07 1C 8A BC 20 EB CE 8E AB EE 31 A2
73 F9 CA 3A 1A FB 0D C1 FE FA F2 6F BD 96 DD 43
52 B6 08 F3 AE BE 19 89 32 26 B0 EA 4B 64 84 82
6B F5 79 BF 01 5F 75 63 1B 23 3D 68 2A 65 E8 91
F6 FF 13 58 F1 47 0A 7F C5 A7 E7 61 5A 06 46 44
42 04 A0 DB 39 86 54 AA 8C 34 21 8B F8 0C 74 67

Підстановка π_3:

68 8D CA 4D 73 4B 4E 2A D4 52 26 B3 54 1E 19 1F
22 03 46 3D 2D 4A 53 83 13 8A B7 D5 25 79 F5 BD
58 2F 0D 02 ED 51 9E 11 F2 3E 55 5E D1 16 3C 66
70 5D F3 45 40 CC E8 94 56 08 CE 1A 3A D2 E1 DF
B5 38 6E 0E E5 F4 F9 86 E9 4F D6 85 23 CF 32 99
31 14 AE EE C8 48 D3 30 A1 92 41 B1 18 C4 2C 71
72 44 15 FD 37 BE 5F AA 9B 88 D8 AB 89 9C FA 60
EA BC 62 0C 24 A6 A8 EC 67 20 DB 7C 28 DD AC 5B
34 7E 10 F1 7B 8F 63 A0 05 9A 43 77 21 BF 27 09
C3 9F B6 D7 29 C2 EB C0 A4 8B 8C 1D FB FF C1 B2
97 2E F8 65 F6 75 07 04 49 33 E4 D9 B9 D0 42 C7
6C 90 00 8E 6F 50 01 C5 DA 47 3F CD 69 A2 E2 7A
A7 C6 93 0F 0A 06 E6 2B 96 A3 1C AF 6A 12 84 39
E7 B0 82 F7 FE 9D 87 5C 81 35 DE B4 A5 FC 80 EF
CB BB 6B 76 BA 5A 7D 78 0B 95 E3 AD 74 98 3B 36
64 6D DC F0 59 A9 4C 17 7F 91 B8 C9 57 1B E0 61

У результаті формується вихідний вектор $r = (r_7, r_6, r_5, r_4, r_3, r_2, r_1, r_0)$: $r_j = \pi_{j \bmod 4}\left[w_j\right]$, де j = 0, 1, …,7.

3. Обчислюється вектор $q = (q_7, q_6, q_5, q_4, q_3, q_2, q_1, q_0)$ за правилом:

$$\begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{pmatrix} = \begin{pmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{pmatrix} \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \end{pmatrix},$$

де елементи матриці (подано у шітнадцятковому вигляді) та векторів r і q інтерпретуються як елементи скінченного поля $GF(2^8)$, яке задане як факторкільце $GF(2)[y]/(p(y))$.

4. Виводиться вихідне значення q, яке інтерпретується як 64-бітовий рядок.

Швидке обчислення вектору q можна реалізувати за правилом:

$$\begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{pmatrix} = \begin{matrix} T_0[w_0] \oplus T_1[w_1] \oplus T_2[w_2] \oplus T_3[w_3] \oplus T_4[w_4] \oplus \\ \oplus T_5[w_5] \oplus T_6[w_6] \oplus T_7[w_7] \end{matrix},$$

де $T_0[a] = \begin{pmatrix} 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \end{pmatrix} \cdot \pi_0[a]$, $T_1[a] = \begin{pmatrix} 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \end{pmatrix} \cdot \pi_1[a]$,

$T_2[a] = \begin{pmatrix} 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \end{pmatrix} \cdot \pi_2[a]$, $T_3[a] = \begin{pmatrix} 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \end{pmatrix} \cdot \pi_3[a]$,

$T_4[a] = \begin{pmatrix} 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \end{pmatrix} \cdot \pi_0[a]$, $T_5[a] = \begin{pmatrix} 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \end{pmatrix} \cdot \pi_1[a]$,

$T_6[a] = \begin{pmatrix} 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \end{pmatrix} \cdot \pi_2[a]$, $T_7[a] = \begin{pmatrix} 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \end{pmatrix} \cdot \pi_3[a]$.

Застосування таблиць-констант $T_i[a]$, $i = 0,1,...,7$ дозволяє значно зменшити кількість операцій, зокрема, функція нелінійної підстановки обчислюється за сім операцій XOR над 64-бітовими рядками.

Множення на α в арифметиці поля $GF(2^{64})$ реалізується за допомогою таблиці передобчислень Mul_α з 256 рядків по 64 бітів в кожному.

Вхід: 64-бітовий рядок w, що представляє елемент поля $GF(2^{64})$.

Вихід: 64-бітовий рядок $w' = w \otimes \alpha$, що представляє елемент поля $GF(2^{64})$.

1. Обчислюється значення $w' = (w << 8) \oplus Mul_\alpha[w >> 56]$, де: $w << 8$ є результатом зсуву ліворуч (в бік старших розрядів) 64-бітового рядка w на 8 розрядів із заповненням молодших розрядів нульовими значеннями; $w >> 56$ є результатом зсуву праворуч (в бік молодших розрядів) 64-бітового рядка w на 56 розрядів із заповненням старших розрядів нульовими значеннями. Вісім молодших розрядів вектору $w >> 56$ інтерпретуються як елемент поля $GF(2^8)$ для індексації таблиці передобчислень Mul_α; Mul_α – таблиця-константа з 256 рядків по 64 бітів в кожному (таблиця передобчислень), $Mul_\alpha[c]$ – 64-бітне значення таблиці передобчислень у рядку з індексом c, де c представляє елемент поля $GF(2^8)$, $Mul_\alpha[c]$ представляє елемент поля $GF(2^{64})$.

2. Виводиться вихідне значення w'.

Множення на α^{-1} в арифметиці поля $GF(2^{64})$ реалізується за допомогою таблиці передобчислень з 256 рядків по 64 бітів в кожному.

Вхід: 64-бітовий рядок w, що представляє елемент поля $GF(2^{64})$.

Вихід: 64-бітовий рядок $w' = w \otimes \alpha^{-1}$, що представляє елемент поля $GF(2^{64})$.

1. Обчислюється значення $w' = (w >> 8) \oplus Mul_{\alpha^{-1}}[w \& \gamma]$, де: $w >> 8$ є результатом зсуву праворуч (в бік молодших розрядів) 64-бітового рядка w на 8 розрядів із заповненням старших розрядів нульовими значеннями; $w \& \gamma$ є результатом побітової кон'юнкції 64-бітового рядка w та 64-бітового рядка γ, який у шістнадцятковому поданні має вигляд $\gamma = 00000000000000FF$. Вісім молодших розрядів вектору $w \& \gamma$ інтерпретуються як елемент поля $GF(2^8)$ для індексації таблиці передобчислень $Mul_{\alpha^{-1}}$;

2. Виводиться вихідне значення w'. Таким чином, генератор СТРУМОК побудовано за SNOW-2.0-подібною схемою підсумовуючого генератора (генератор SNOW-2.0 визначено в ДСТУ ISO/IEC 18033-4:2015). Він використовує 256-бітний вектор ініціалізації та 256-бітний або 512-бітний секретний ключ. Генератор забезпечує високий та надвисокий рівні стійкості (див. табл. 3) та призначений для забезпечення конфіденційності інформації під час її оброблення із врахуванням можливого застосування квантового криптографічного аналізу.

Це є унікальним українським рішенням, яке забезпечує високу швидкість криптоперетворення (див. табл 4) та надзвичайно високі показники безпеки, навіть з урахуванням можливого застосування в пост-квантовому середовищі, в умовах ведення інформаційних та гібридних війн.

Таблиця 3

Встановлені рівні захисту

Генератор ключових потоків, встановлений рівень захисту	Довжина ключа	Обчислювальна складність для найкращої відомої атаки	Обчислювальна складність квантового криптографічного аналізу
СТРУМОК-256, високий	256	2^{256}	2^{128}
СТРУМОК-512, надвисокий	512	2^{512}	2^{256}

Основні результати з розробки, дослідження та впровадження в Україні національних стандартів асиметричного КЗІ для пост-квантового застосування.

Для побудови надійних та безпечних моделей, методів, протоколів та алгоритмів КЗІ, стійких як до класичних, так і до квантових технологій криптоаналізу, необхідно застосовувати нові криптографічні примітиви, стійкість яких базується на застосуванні односторонніх математичних функцій, складність обернення яких не зменшується навіть у разі використання відомих квантових алгоритмів вирішення складних теоретико-обчислювальних задач.

Таблиця 4

Швидкість генерації ключових потоків

	Intel Core i3-4005U 1.7 GHz, Windows 10 x64	Intel Core i5-7200U 2.5 GHz, Windows 10 x64	Intel Core i7-7700 3,6 GHz, Windows 10 x64
SNOW 2.0-128	4,2 Гбіт/с	8,0 Гбіт/с	10,6 Гбіт/с
SNOW 2.0-256	4,2 Гбіт/с	8,0 Гбіт/с	10,6 Гбіт/с
СТРУМОК-256	6,8 Гбіт/с	12,8 Гбіт/с	17,4 Гбіт/с
СТРУМОК-512	6,8 Гбіт/с	12,8 Гбіт/с	17,4 Гбіт/с

Національний стандарт ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів» установлює криптографічний алгоритм асиметричного шифрування та інкапсуляції ключів для забезпечення конфіденційності, цілісності, доступності, неспростовності та криптоживучості (як додаткової послуги) інформації та ключів під час їх оброблення [16]. У стандарті описано алгоритм асиметричного шифрування та інкапсуляції ключів, який використовує перетвореннях у кільці та скінченому полі для асиметричного поблокового шифрування та інкапсуляції ключів з використанням асиметричних пар ключів – для зашифрування з використанням відкритого ключа отримувача та інкапсуляції з використання секретного ключа сеансу інкапсуляції відправника. З використанням відповідних відкритого та секретного ключів отримувача та відправника обчислюється та встановлюється секретний ключ для блокового чи потокового симетричного шифрування інформації, отже стандарт визначає асиметричний блоковий шифр та протокол інкапсуляції ключів, які застосовуються для подальшого вироблення та встановлення ключів блокового чи потокового симетричного шифрування (за класифікацією ДСТУ ISO/IEC 18033-2:2015).

В алгоритмі асиметричного шифрування використовується асиметрична пара ключів – відкритий ключ для зашифрування блоків інформації (даних) відправником, а особистий (секретний) ключ – для розшифрування зашифрованих блоків отримувачем.

В алгоритмі (протоколі) інкапсуляції ключів також використовується асиметрична пара ключів – особистий (секретний) ключ сеансу – для інкапсуляції ключа сеансу відправником, а відкритий ключ сеансу – для декапсуляції сеансового ключа отримувачем.

Отримувач на основі свого секретного (особистого) ключа розшифрування та декапсульованого ключа сеансу відправника, а відправник на основі відкритого ключа зашифрування отримувача та свого секретного ключа сеансу, виробляють спільну таємницю (спільний ключ). В подальшому спільний ключ може використовуватись для шифрування інформації (даних) в каналах зв'язку при обміні інформацією.

Інкапсуляція ключа представляє процес криптографічного перетворення ключа сеансу та інших даних з метою забезпечення їх конфіденційності, цілісності (справжності) та криптоживучості, а також узгодження ключа симетричного шифрування даних між відправником та отримувачем в подальшому. Декапсуляція представляє собою процес перевірки цілісності та справжності інкапсульованого ключа сеансу зв'язку та узгодження ключа захисту даних між отримувачем та відправником.

Шифрування та інкапсуляція ключів здійснюється на основі математичних перетворень в кільці поліномі над скінченим полем.

При розробленні стандарту враховані вимоги щодо забезпечення криптографічної стійкості проти спеціальних атак на основі витоку по технічним каналам, а також потенційних класичних та квантових атак, в тому числі у перехідний та постквантовий періоди. Стандарт розроблено з урахуванням досвіду створення та застосування стандартів ДСТУ ISO/IEC 18033-2:2015, ANSI X9.98-2010 та результатів, що представлені в [1-10].

Цей стандарт може використовуватись під час розробки систем, комплексів та засобів криптографічного захисту інформації при наданні користувачам послуг конфіденційності, цілісності, неспростовності, доступності та криптоживучості ключів, що узгоджуються відправником та отримувачем, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, в тому числі для захисту від спеціальних атак, а також у перехідний та постквантовий періоди.

Режими роботи та функції криптографічного захисту. Стандарт, у залежності від рівня криптографічної стійкості проти класичних та квантових атак, яку необхідно забезпечити, може застосовуватись в трьох режимах роботи:

- режим Скеля – KEM 256/128 – 256 біт захисту від класичних атак та 128 біт захисту від

квантових атак, а також захисту від спеціальних атак;

- режим Скеля – KEM 384/192 – 384 біт захисту від класичних атак та 192 біт захисту від квантових атак, а також захисту від спеціальних атак;

- режим Скеля – KEM 512/256 – 512 біт захисту від класичних атак та 256 біт захисту від квантових атак, а також захисту від спеціальних атак.

Також в кожному із режимів роботи можуть використовуватись окремо такі криптографічні перетворення:

- незалежний алгоритм (функція) асиметричного шифрування;

- протокол інкапсуляції ключів (функція), що ґрунтується на використанні функції асиметричного шифру;

- механізм (функція) симетричного шифрування та автентифікації, що ґрунтується на функціях асиметричного шифрування та інкапсуляція ключів.

В кожному із режимів роботи за рахунок застосування криптографічних перетворень в кільцях поліномів та скінчених полях забезпечується надання послуг конфіденційності, цілісності, справжності, доступності та криптографічної живучості ключа сеансу зв'язку та його узгодження між відправником та отримувачем.

Прийнятий національний стандарт ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів» заплановано до впровадження протягом 2021 року із наданням чинності з 01 січня 2021 року, отже в цій роботі докладний опис відповідних алгоритмів не наводиться. Стандарт планується використовувати під час розробки комплексів, систем та засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також в разі модернізації наявних систем для заміни асиметричних режимів шифрування та інкапсуляції ключів згідно з ДСТУ ISO/IEC 18033-2:2015, в тому числі у постквантовий період, при використанні стандарту забезпечується захист від спеціальних атак сторонніми каналами, в тому числі криптографічна стійкість у постквантовий період.

ВИСНОВКИ

Протягом 2014-2020 р. в Україні розроблено, досліджено, організовано прийняття та впроваджено низку національних криптографічних стандартів (ДСТУ 7624:2014; ДСТУ 7564:2014; ДСТУ 8845:2019; ДСТУ 8961:2019), які відповідають найжорсткішим вимогам надійності та безпеки, встановленим NIST США до постквантових криптографічних алгоритмів, в тому числі до асиметричного шифрування та інкапсуляції ключів (ДСТУ 8961:2019).

Безпосередньо за участю авторів цієї роботи виконано більше 100 НДР та ДКР, в тому числі за державним оборонним замовленням, господарчими договорами та за держбюджетним замовленням. За отриманими результатами розроблено та впроваджено основні елементи загальнонаціональної системи КЗІ: програмно-технічні комплекси акредитованих центрів сертифікації ключів (АЦСК) Міністерства зборів та податків, Укрзалізниці, Державної митної служби, Державної автомобільної інспекції, МОН України, тощо, АЦСК центрального засвідчувального органу (ЦЗО), тощо. Авторами розроблено та впроваджено в дію на базі державного підприємства Інформресурс систему захисту інформації МОН України. Розроблено та функціонують АЦСК та системи КЗІ більше 10 комерційних банків (Укрсіббанк, Укрсоцбанк, Приватбанк та інші). Розроблено та введено в дію Інтегровану систему електронної ідентифікації ID.GOV.UA, підсистему КЗІ Єдиного порталу державних послуг Дія, тощо. За результатами досліджень підготовлено серію наукових та навчально-методичних робіт (підручників, навчальних посібників та монографій), які вже впроваджено в навчальний процес провідних ВНЗ України за спеціальністю 125 - кібербезпека.

ЛІТЕРАТУРА

[1] *Post-Quantum Cybersecurity Resources* [Електронний ресурс] – Режим доступу до ресурсу: https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/.

[2] *NISTIR 8105 Report on Post-Quantum Cryptography* [Електронний ресурс] – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[3] *Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges* [Електронний ресурс] – Режим доступу до ресурсу: https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf.

[4] *Neal Koblitz and Alfred J. Menezes. A Riddle Wrapped in an Enigma* [Електронний ресурс] – Режим доступу до ресурсу: https://eprint.iacr.org/ 2015/1018.pdf.

[5] *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms* [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms.

[6] *NISTIR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process* [Електронний ресурс] – Режим доступу до ресурсу: https://nvlpubs.nist.gov/ nistpubs/ir/2020/NIST.IR.8309.pdf.

[7] *11th International Conference, PQCrypto 2020*, Paris, France, April 15–17, 2020, Proceedings [Електронний ресурс] – Режим доступу до ресурсу: https://link.springer.com/book/10.1007/978-3-030442 23-1.

[8] Kris Gaj. *Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using FPGAs*. [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/ Projects/post-quantum-cryptography/documents/round-3/ seminars/oct-2020-gaj-kris-resentation.pdf.

[9] *Round 3 Submissions* [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/ projects/post-quantum-cryptography/round-3-submissions.

[10] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner and Thomas Vidick. *Practical device-independent quantum cryptography via entropy accumulation*. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov /pmc/articles/PMC5792631/.

[11] *Держспецзв'язку впроваджує нові стандарти криптографічного захисту інформації* [Електронний ресурс] – Режим доступу до ресурсу: https://www.kmu.gov.ua/news/247952015.

[12] *Про прийняття національних стандартів України, гармонізованих з європейськими стандартами, міжнародних стандартів як національних стандартів України, затвердження національних стандартів України, скасування міждержавних стандартів в Україні та внесення зм* [Електронний ресурс] – Режим доступу до ресурсу: https://zakon. rada Про прийняття та скасування національних стандартів, прийняття змін до національних стандартів, скасування міждержавного стандарту. https://zakon.rada.gov.ua/rada/show/v0085774-19#Text.gov.ua/rada/show/v1431731-14#Text.

[13] *Про прийняття та скасування національних стандартів, прийняття змін до національних стандартів, скасування міждержавного стандарту* [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua /rada/show/v0085774-19#Text.

[14] *Каталог НД України* [Електронний ресурс] – Режим доступу до ресурсу: http://csm.kiev.ua /nd/nd.php?z=%D0%94%D0%A1%D0%A2%D0%A3+8845%3A2019&st=0&b=1.

[15] *Про прийняття та скасування національних стандартів* [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/v0465774-19#Text.

СТАНДАРТИЗАЦИЯ СИСТЕМ, КОМПЛЕКСОВ И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРИМЕНЕНИЯ В ПОСТ-КВАНТОВОЙ СРЕДЕ

Криптографическая защита информации (КЗИ) является важной составляющей информационной безопасности государства, непосредственно связанной с преодолением современных проблем и вызовов в кибернетическом пространстве Украины, новых угроз информационной безопасности в критических инфраструктурах в оборонной и сфере безопасности, промышленности, банковском секторе, экономике и т. Особую опасность в этом смысле представляют новые риски, связанные с разработкой и стремительным внедрением современных и перспективных информационных технологий, способных в корне изменить архитектуру информационных систем, существующие парадигмы, стали принципы построения и математические основы современных средств криптографической защиты. В частности, появление и стремительное совершенствование новых вычислительных средств, основанных на принципах и эффектах квантовой физики (т.н. универсальных квантовых компьютеров) ставит под угрозу само существование действующих ныне и стандартизированных на национальном и международном уровнях механизмов (протоколов, алгоритмов и средств) асимметричной криптографии.

Ключевые слова: квантовые вычислители, крипографические алгоритмы, информационная безопасность, информационная безопасность, информационные системы.

STANDARDIZATION OF SYSTEMS, COMPLEXES AND MEANS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION FOR APPLICATION IN POST-QUANTUM ENVIRONMENT

Cryptographic information protection (CRC) is an im-

portant component of information security of the state, directly related to overcoming modern problems and challenges in the cyberspace of Ukraine, new threats to information security in critical infrastructures in defense and security, industry, banking, economy, etc. Particularly dangerous in this sense are the new risks associated with the development and rapid implementation of modern and advanced information technologies that can radically change the architecture of information systems, existing paradigms, stable principles of construction and mathematical foundations of modern CCI tools. In particular, the emergence and rapid improvement of new computing tools based on the principles and effects of quantum physics (so-called universal quantum computers) threatens the very existence of existing and standardized at the national and international levels mechanisms (protocols, algorithms and tools) asymmetric cryptography.

Keywords: quantum computers, cryptographic algorithms, information security, information systems.

Корченко Анна Олександрівна, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету, доктор технічних наук, доцент.
E-mail: annakor@ukr.net.
Orcid ID: 0000-0003-0016-1966.

Корченко Анна Александровна, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета, доктор технических наук, доцент.

Korchenko Anna, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University, Doctor of Technical Sciences, Associate Professor.

Іванченко Євгенія Вікторівна, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету, кандидат технічних наук, доцент.
E-mail: evivancenko@gmail.com.
Orcid ID: 0000-0003-3017-5752.

Иванченко Евгения Викторовна, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета, кандидат технических наук, профессор.

Ivanchenko Yevheniya, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University, Candidate of Technical Sciences, Associate Professor.

Кошкіна Наталія Василівна, старший науковий співробітник відділу оптимізації чисельних методів, Інститут кібернетики імені В.М. Глушкова НАН України, доктор технічних наук, старший науковий співробітник.
E-mail: nata.koshkina@gmail.com.
Orcid ID: 0000-0001-5180-2255.

Кошкина Наталья Васильевна, старший научный сотрудник отдела оптимизации численных методов, Институт кибернетики имени В.М. Глушкова НАН Украины, доктор технических наук, старший научный сотрудник.

Koshkina Natalia, Senior Research Fellow, Department of Optimization of Numerical Methods, Institute of Cybernetics Glushkova NAS of Ukraine, Doctor of Technical Sciences, Senior Researcher.

Кузнецов Олександр Олександрович, професор кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій» доктор технічних наук, професор.
E-mail: kuznetsov@karazin.ua.
Orcid ID: 0000-0003-2331-6326.

Кузнецов Александр Александрович, профессор кафедры безопасности информационных систем и технологий факультета компьютерных наук Харьковского национального университета имени В. Н. Каразина, по-Ступник главного конструктора частного акционерного общества «Институт информационных технологий» доктор технических наук, профессор.

Kuznetsov Oleksandr, Professor of the Department of Information Systems Security and Technologies, Faculty of Computer Science, VN Karazin Kharkiv National University, Deputy Chief Designer of the Private Joint-Stock Company "Institute of Information Technologies", Doctor of Technical Sciences, Professor.

Качко Олена Григорівна, професор кафедри програмної інженерії факультету комп'ютерних наук Харківського національного університету радіоелектроніки, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій» кандидат технічних наук, професор.
E-mail: ekachko@gmail.com.
Orcid ID: 0000-0001-9249-0497.

Качко Елена Григорьевна, профессор кафедры программной инженерии факультета компьютерных наук Харьковского национального университета радиоэлектроники, заместитель главного конструктора частного акционерного общества «Институт информационных технологий» кандидат технических наук, профессор.

Kachko Olena, Professor of the Department of Software Engineering, Faculty of Computer Science, Kharkiv National University of Radio Electronics, Deputy Chief

Designer of the Private Joint-Stock Company "Institute of Information Technologies", Candidate of Technical Sciences, Professor.

Потій Олександр Володимирович, заступник Голови Державної служби спеціального зв'язку та захисту інформації України доктор технічних наук, професор.
E-mail: potii.oleksandr@gmail.com.
Orcid ID: 0000-0002-2366-0541.
Потий Александр Владимирович, заместитель Председателя Государственной службы специальной связи и защиты информации Украины, доктор технических наук, профессор.
Potiy Oleksandr, Deputy Head of the State Service for Special Communications and Information Protection of Ukraine, Doctor of Technical Sciences, Professor.

Онопрієнко Віктор Васильович, генеральний директор приватного акціонерного товариства «Інститут інформаційних технологій», кандидат технічних наук, старший науковий співробітник.
E-mail: kuznetsov@karazin.ua.
Orcid ID: 0000-0001-5681-3412.

Оноприенко Виктор Васильевич, генеральный директор частного акционерного общества «Институт информационных технологий», кандидат технических наук, старший научный сотрудник.
Onoprienko Viktor, General Director of the Private Joint-Stock Company "Institute of Information Technologies", Candidate of Technical Sciences, Senior Researcher.

Бобух Всеволод Анатолійович, начальник відділу апаратних засобів захисту інформації приватного акціонерного товариства «Інститут інформаційних технологій», кандидат технічних нау
E-mail: bobukhv@iit.kharkov.ua.
Orcid ID: 0000-0002-1175-5092.
Бобух Всеволод Анатольевич, начальник отдела аппаратных средств защиты информации частного акционерного общества «Институт информационных технологий», кандидат технических наук
Bobukh Vsevolod, Head of the Department of Information Protection Hardware of the Private Joint-Stock Company "Institute of Information Technologies", Candidate of Technical Sciences

DOI: 10.18372/2410-7840.22.14977
УДК 004.94

DEVELOPMENT OF UNCLEAR CRITERIA FOR DETERMINING THE SIGNIFICANCE OF A COMPOSITE SOCIAL PROFILE INFORMATION

Mykhailo Mozhaiev, Pavlo Buslov, Viktoriia Shvedun

Summary. The results of development of fuzzy criteria for determination of significance of composite information of social profile are presented. The simulation is carried out using OSINT technology - the technology of legal acquisition and use of information from open sources. As a result of the research, the parameters affecting the significance of individual characteristics of the social profile are selected and their characteristics are determined. The information of varying degrees of structurality is processed in the course of performing of the task of social profiling. At the same time, the following data models are used: network one - for storing the data of the final social profile, and presenting them in the form of graphs; relational one - for storing the information map of the social profile; post-shooting and NoSQL one - for storing unstructured source data and dynamic content, including multimedia. The conceptual model of presentation of these social profiles can be expanded and brought into line with the complex and mathematical models of the digital social environment. In the future, it is necessary to disclose the elements and relationships of the four basic categories of the infological model of presenting the results of social profiling. A new model of fuzzy significance coefficient of social profile parameters is obtained, the difference of which is the possibility of taking into account both formalized objective and difficult-to-interpret subjective indicators for evaluating the initial information of the SP. The advantage of using the significance criterion over the involvement of experts is the lower time spent on analyzing large amounts of data while maintaining the level of objectivity of the assessment. Consideration the diversity of the digital social environment is the next step.
Key words: *information technologies, fuzzy criteria, information from open sources, social portrait, formalization of criteria, information model, infological model.*

INTRODUCTION

Currently, the possession of information on the social profile of both the individual and the social group as a whole is of significant interest in most areas of human and social activity: economics, education, politics, security, comfortable living conditions ensuring, etc. Therefore, formation of a social portrait of an individual, a group, as well as the who-