УДК 519.713

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ПОТОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ (ЗА РЕЗУЛЬТАТАМИ ВИКОНАННЯ ПРОЕКТУ eSTREAM)

І.Д. ГОРБЕНКО, А.В. НЕЙВАНОВ

Дана робота присвячується сучасним досягненням в області потокових симетричних шифрів. Ми розглядаємо переможців проекту eSTREAM, розробляємо критерії та показники оцінки стійкості потокових симетричних шифрів та застосовуємо до них методику ухвалення рішень на множині альтернативних варіантів з ціллю відібрати найкращі алгоритми потокового шифрування.

The paper is devoted to modern developments in the field of stream symmetrical ciphers. It considers the winners of eSTREAM project and develop criteria and indicators of assessing the security of stream symmetric cipher as well as applies the method of decision making on a set of alternatives in order to select the best stream encryption algorithms.

Після більш ніж трьох років проект eSTREAM підійшов до кінця. На електронному ресурсі проекту з'явився фінальний збір робіт, які містить найбільш успішні потокові симетричні шифри й деякі аспекти відкритих розрахунків. Основною метою проекту eSTREAM була стимуляція роботи в області потокових симетричних шифрів. І в цьому організатори добилися успіху. Вони склали перелік з потокових симетричних шифрів, що витримали три етапи конкурсу. Самих стійких, на думку криптографів, які в наслідку можуть бути розглянуті як стандарти, рекомендовані до застосування та випробовування. Метою цієї статті є добір кращих алгоритмів ПСШ та аналіз їх властивостей.

1. МЕТОДИКА УХВАЛЕННЯ РІШЕННЯ НА МНОЖИНІ АЛЬТЕРНАТИВНИХ ВАРІАНТІВ

Відповідно до положень загальної теорії прийняття рішень, під ефективністю «функціонування» алгоритму шифрування будемо розуміти ступінь відповідності отриманих результатів якості функціонування R_p необхідним $R_н$:

$$C = < R_p , R_н >.$$

Необхідним результатом функціонування $R_н$ є рівень (ступінь) забезпечення конфіденційності шляхом реалізації механізму шифрування. Досягнутим результатом функціонування R_p є реальний рівень забезпечення конфіденційності. Оцінка того, наскільки повно реалізована функція конфіденційності або, іншими словами, наскільки R_p відповідає $R_н$, здійснюється за допомогою великого набору показників і критеріїв, що відбивають рівень виконання алгоритмом окремих складових загальної функціональної задачі.

На сьогоднішній день відносно потокових симетричних шифрів не існує систематизованого підходу для перетворення множини значень показників у єдиний показник, яким можна охарактеризувати ефективність функціонування схеми шифрування. Розроблювачі шифрів пропонують різні набори показників, що характеризують окремі сторони шифрів, але це не дозволяє представити картину в цілому. Для рішення таких задач на практиці часто застосовуються елементи теорії нечітких множин. Розглянемо деякі елементи даної теорії.

Нехай U – повна множина, що охоплює всі об'єкти деякого класу. Нечітка підмножина F множини U, що надалі будемо називати нечіткою множиною, визначається через функцію приналежності $\mu_F(u)$, $u \in U$. Ця функція відображає елементи u_i множини U на множину ірраціональних чисел відрізка [0,1], що вказують ступінь приналежності кожного елемента нечіткій множині F.

Якщо повна множина U складається з кінцевого числа елементів u_i, $i = 1, 2, ..., n,$ то нечітку множину F можна представити в такому вигляді:

$$F = \mu_F(u_1)/u_1 + \mu_F(u_2)/u_2 + ... + \mu_F(u_n)/u_n.$$

Таким чином, для вирішення задачі вибору алгоритму шифрування можна скористатися елементами теорії нечітких множин. Експертні оцінки альтернативних варіантів за визначеним умовним критерієм можуть бути представлені як нечіткі множини або числа, виражені за допомогою функцій приналежності. Розглянемо одну з математичних постановок задачі прийняття рішень на основі теорії нечітких множин.

У даному випадку критерії визначають деякі поняття, а оцінки альтернатив являють собою ступені відповідності цим поняттям. Нехай є множина альтернатив $A = \{a_1, a_2, ..., a_m\}$ і множина критеріїв $C = \{C_1, C_2, ..., C_n\}$, при цьому оцінки альтернатив по кожному i-му критерію представлені нечіткими множинами:

$$C_i = \left\{\mu_{C_i}(a_1)/a_1 + \mu_{C_i}(a_2)/a_2 + ... + \mu_{C_i}(a_m)/a_m\right\}. \quad (1)$$

Правило вибору кращої альтернативи можна представити як перетинання нечітких множин:

$$D = C_1 \cap C_2 \cap ... \cap C_n.$$

Операція перетинання нечітких множин може бути реалізована різними способами. Іноді перетинання виконується як множення, але частіше ця операція виконується як взяття мінімуму [2] для різних альтернатив:

$$\mu_D(a_j) = \min_{i=1,...,n} \mu_{C_i}(a_j), j = 1,...,m .$$

Кращою вважається альтернатива a^*, що має найбільше значення функції приналежності:

$$\mu_D(a^*) = \max_{j=1,\ldots,m} \mu_D(a_j).$$

У випадку порівняння алгоритмів шифрування всі критерії мають різну важливість, тому їх внесок у загальне рішення можна представити як зважене перетинання (2):

$$D = C_1^{\beta_1} \cap C_2^{\beta_2} \cap \ldots \cap C_n^{\beta_n}, \qquad (2)$$

де β_i – вагові коефіцієнти відповідних критеріїв, що повинні задовольняти умовам:

$$\beta_i \geq 0; i = 1,\ldots,n; (1/n)\sum_{i=1}^{n} \beta_i = 1.$$

Коефіцієнти відносної важливості визначаються з використанням процедури попарного порівняння критеріїв.

Розглянемо цю процедуру, використовуючи метод попарного порівняння.

Метод попарного порівняння елементів (2) можна описати в такий спосіб. Будується множина матриць парних порівнянь. Парні порівняння проводяться в термінах домінування одного елемента над іншим. Отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали (див. табл. 1).

Заповнення квадратних матриць парних порівнянь здійснюється за таким правилом. Якщо елемент E_i домінує над елементом E_j, то клітка матриці, що відповідає рядку E_i і стовпцю E_j, заповнюється цілим числом, а клітка, що відповідає рядку E_j і стовпцю E_i, заповнюється зворотним йому числом.

Для одержання кожної матриці експерт або особа, що приймає рішення, виносить $n(n\text{-}1)/2$ суджень (тут n – порядок матриці парних порівнянь).

Розглянемо в загальному вигляді приклад формування матриці парних порівнянь.

Нехай E_1, E_2, ..., E_n – множина з n елементів (альтернатив) і $\nu_1, \nu_2, \ldots, \nu_n$ – відповідно їх ваги або інтенсивності. Порівняємо попарно вагу або інтенсивність, кожного елемента з вагою, або інтенсивністю, будь-якого іншого елемента множини стосовно загальної для них властивості або мети. У цьому випадку матриця парних порівнянь $[E]$ має такий вигляд:

$$[[E] = \begin{array}{|c|c|c|c|c|} \hline & E_1 & E_2 & \cdots & E_n \\ \hline E_1 & \nu_1/\nu_1 & \nu_1/\nu_2 & \cdots & \nu_1/\nu_n \\ \hline E_2 & \nu_2/\nu_1 & \nu_2/\nu_2 & \cdots & \nu_2/\nu_n \\ \hline \ldots & \ldots & \ldots & \ldots & \ldots \\ \hline E_n & \nu_n/\nu_1 & \nu_n/\nu_2 & \cdots & \nu_n/\nu_n \\ \hline \end{array}$$

При проведенні попарних порівнянь варто відповідати на такі питання: який із двох порівнюваних елементів важливіше або має більший вплив, який більш ймовірний і який більш кращий. При порівнянні критеріїв звичайно запитують, який із критеріїв більш важливий; при порівнянні альтернатив стосовно критерію – яка з альтернатив більш краща або більш ймовірна (2).

Ранжирування елементів, що аналізуються з використанням матриці парних порівнянь $[E]$, здійснюється на підставі головних власних векторів, що одержуються у результаті обробки матриць (2).

2. КРИТЕРІЇ ТА ПОКАЗНИКИ ОЦІНКИ СТІЙКОСТІ ПОТОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Наведені вище результати дозволяють виконати порівняння шифрів та вибір одного з них з використанням розвинутої методики.

Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь. У такому розумінні узагальнений критерій порівняння алгоритмів шифрування можна представити у вигляді двох складових: безумовного та умовного критеріїв. Кожен з цих критеріїв є залежним від відповідного набору тих чи інших ознак.

Таблиця 1

Ступінь значимості	Визначення	Пояснення
1	Однакова значимість	Дві дії вносять однаковий вклад у досягнення мети
3	Деяка перевага значимості однієї дії над іншою (слабка значимість)	Існують розуміння на користь переваги однієї з дій, однак ці розуміння недостатньо переконливі
5	Істотна або сильна значимість	Є надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значимість	Переконливе свідчення на користь однієї дії перед іншою
9	Абсолютна значимість	Свідчення на користь переваги однієї дії іншій найвищою мірою переконливі
2,4,6,8	Проміжні значення між двома сусідніми судженнями	Ситуація, коли необхідно компромісне рішення
Зворотні величини приведених вище ненульових величин	Якщо дії i при порівнянні з дією j приписується одне з визначених вище ненульових чисел, то дії j при порівнянні з дією i приписується зворотне значення	Якщо погодженість була постульована при одержанні N числових значень для утворення матриці

Оцінку претендентів будемо виконувати в два етапи. На першому етапі алгоритми-кандидати перевірятимуться на відповідність безумовним критеріям. Оскільки безумовні критерії допускають вибір тільки стійких алгоритмів, то кожний алгоритм, що відповідає безумовним критеріям, потенційно може використовуватися.

До безумовних критеріїв віднесено ті критерії (показники), виконання яких є обов'язковим для шифру.

Потоковий симетричний шифр повинен безумовно володіти наступними властивостями (задовольняти безумовному критерію).

1. Захищеність від усіх відомих та потенційно можливих криптоаналітичних атак, де під захищеністю розуміється той факт, що усі криптоаналітичні атаки мають складність більшу ніж атака типу «груба сила», що будемо позначати $K_{б1}$.

2. Статистична безпечність алгоритму шифрування, під якою розуміється статистична незалежність зашифрованих повідомлень функції виходу та гам шифруючих від генератора ключового потоку. Цю складову критерію будемо позначати $K_{б2}$.

3. Надійність математичної бази в змісті відсутності можливостей здійснювати атаки універсальне розкриття за рахунок недосконалості або закладеної навмисної специфічної математичної бази. При цьому вважається, що атака універсальне розкриття має складність набагато меншу ніж складність атаки «груба сила». Будемо позначати цю складову критерію як $K_{б3}$.

4. Практична захищеність алгоритму шифрування від силових атак, яка може досягатись на основі використання симетричних криптоперетворень з рівнем безпеки не менш ніж 128 бітів. Будемо позначати цю складову критерію як $K_{б4}$.

5. Відсутність слабких початкових ключів та підозр на існування ключів, при яких складність криптоаналітичної атаки є меншою ніж складність атаки груба сила. Цю складову критерію позначимо через $K_{б5}$.

6. Складність прямого та зворотного перетворень не перевищують допустимої величини, крім того, складність генерації ключового потоку не перевищує заданої. Цю складову критерію позначимо через $K_{б6}$.

У використаних позначеннях часткових критеріїв нижній індекс означає номер часткового критерію.

Оскільки наведені часткові критерії є безумовними, то критерієм добору є логічна змінна Так/Ні (1/0).

Використавши позначення булевої алгебри, можемо записати:

$$(K_{б1}, K_{б2}, K_{б3}, K_{б4}, K_{б5}, K_{б6}) \in \{1,0\}.$$

З урахуванням наведених вище критеріїв функція відповідності ПСШ безумовному критерію (тобто усім $K_{б1} - K_{б6}$ частковим критеріям) може бути записано як

$$f_{бк}(\text{шифр}) = K_{б1} \wedge K_{б2} \wedge K_{б3} \wedge K_{б4} \wedge K_{б5} \wedge K_{б6}, \qquad (3)$$

де символ «$\wedge$» позначає операцію кон'юнкції булевих змінних.

Функція $f_{бк}(\text{шифр}) \in \{0,1\}$ і при $f_{бк}(\text{шифр}) = 1$ оцінюємий алгоритм шифрування відповідає безумовному критерію.

Другою складовою загального критерію пропонується узагальнений критерій переваги. Цей критерій є умовним, в якості його складових пропонується використовувати наступні часткові умовні критерії (табл. 2).

Таблиця 2

Часткові умовні критерії узагальненого критерію переваги $K_у$

№	Критерій	Позначення
1	Можливість і умови вільного поширення алгоритму в Україні з урахуванням національного та міжнародного законодавства	$K_{у1}$
2	Рівень довіри до шифру	$K_{у2}$
3	Перспективність застосування алгоритму шифрування	$K_{у3}$
4	Складність програмної реалізації	$K_{у4}$
5	Гнучкість алгоритму шифрування	$K_{у5}$

В подальшому будемо вважати, що оцінка по кожному із часткових критеріїв здійснюється завдяки використанню показників $K_{у1}$, $K_{у2}$, $K_{у3}$, $K_{у4}$, $K_{у5}$, де індекс $i = \overline{1,5}$ означає номер часткового критерію.

Оцінку та порівняльний аналіз алгоритмів шифрування будемо здійснювати за допомогою наведених вище безумовного та умовного критеріїв. Кожен з цих критеріїв в свою чергу визначається через сукупність часткових критеріїв. Кожен з цих часткових критеріїв будемо застосовувати для прийняття рішення, використовуючи наступні показники або сукупність показників:

1. Захищеність від усіх відомих атак. Для визначення цього критерію будемо спиратися на відомі джерела, присвячені пошуку криптоаналітичних атак на тій чи інших шифр. За результатами експертних оцінок $K_{б1}$ приймає значення 1 чи 0.

2. Оцінку статистичної безпечності пропонується здійснювати використовуючи ряд підходів, що закладені для статистичного тестування у пакетах NIST STS та Crypt-X.

На основі аналізу результатів тестування згідно цих методик експертами приймається рішення $K_{б2} = 1$ чи 0 і, відповідно, алгоритм залишається для подальшого аналізу чи відкидається.

3. Оцінку надійності математичної бази можна здійснювати на основі експертних оцінок спеціалістів-криптологів. При цьому повинна враховуватись ступінь відкритості проектування та дослідження алгоритму шифрування. Основним же фактором є можливість еквівалентного (альтернативного) представлення криптографічних перетворень та виконання криптоаналізу з меншою або суттєво зменшеною складністю вказаних перетворень. В результаті приймається рішення $K_{б3} = 1$ чи 0.

4. Оцінку практичної захищеності алгоритму шифрування від силових атак можна здійснювати використовуючи розмір простору дозволених ключів. Виходячи з цього критерію, будемо розглядати шифри, для яких розмір ключа не нижче ніж 128 бітів. В інших випадках $K_{б4} = 0$.

5. Оцінка відсутності чи наявності слабких початкових ключів є однією з найбільш складних задач. Її розв'язок повинний здійснюватись на основі експертної оцінки як алгоритму прямого так і зворотного криптографічних перетворень і перш за все алгоритму генерації ключового потоку. Перша задача експертної оцінки повинна здійснюватись на основі визначення чи не є деякі ключі слабкими при застосуванні того чи іншого методу криптоаналізу. Основними при цьому є такі методи – диференційний криптоаналіз, лінійний криптоаналіз, інтерполяційне вторгнення, інтегральна атака, вторгнення з частковим угадуванням ключа, вторгнення з використанням зв'язаних ключів, пошук лазівок, вторгнення на основі обробки збоїв. У результаті виконання аналізу може бути прийнято рішення про наявність чи відсутність слабких початкових ключів і відповідно $K_{б5} = 1$ чи $K_{б5} = 0$.

6. Оцінка складності процедур встановлення ключа, встановлення мітки часу, процедури генерації ключового потоку, а також зашифровування пакету (в тактах процесора) може бути здійснена на основі даних проекту eSTREAM, наведених у [1]. В [1] наведено дані щодо складності перетворень різних шифрів, що реалізовані під найбільш поширені сьогодні процесори. Серед шифрів, що будуть аналізуватися, будемо відкидати найбільш повільні шифри. Для цих шифрів $K_{б6} = 0$, для інших – $K_{б6} = 1$.

3. ПОСЛІДОВНІСТЬ АНАЛІЗУ ТА ВИБОРУ АЛГОРИТМУ ПОТОКОВОГО ШИФРУВАННЯ

Виконується оцінка алгоритму потокового шифрування з використанням умовних критеріїв на основі теорії нечітких множин. Будемо використовувати показник (2), що може бути представлений як

$$D = C_1^{\beta_1} \cap C_2^{\beta_2} \cap ... \cap C_n^{\beta_n},$$

де C_i – числові значення приватних критеріїв узагальненого умовного критерію, отримані методом експертної оцінки і представлені нечіткими множинами (2); β_i – ваговий коефіцієнт i-го критерію, отриманий за допомогою матриці попарних порівнянь відповідно описаного в (2).

Таким чином, вибір алгоритму шифрування пропонується здійснювати в такій послідовності:

1. Визначаються числові значення показників $K_{б1}$, $K_{б2}$, $K_{б3}$, $K_{б4}$, $K_{б5}$, $K_{б6}$, що входять до безумовної функції (3) $f_{бк}(A_i)$.

2. Визначаються значення функцій $f_{I:}(A_i)$. Якщо $f_{бк}(A_i)$ i-того алгоритму приймає значення «1», то відповідний алгоритм задовольняє безумовному узагальненому критерію. Про це також свідчить значення функції $f_{бк}(A_i)$ = «1» (істина).

3. Для алгоритмів, що задовольняють узагальненому безумовному критерію, тобто $f_{бк}(A_i) = 1$, згідно часткових умовних критеріїв обчислюються значення часткових умовних показників $K_{у1}$, $K_{у2}$, $K_{у3}$, $K_{у4}$ та $K_{у5}$.

4. Обчислюють значення узагальненого умовного показника $K_у$ для кожного із альтернативних кандидатів.

5. На основі порівняння значень $K_у$ для різних шифрів робиться висновок про більш кращі властивості одного чи іншого алгоритму.

4. МЕТОДИКА ОЦІНКИ СТІЙКОСТІ ПСШ

4.1 Порівняльний аналіз алгоритмів шифрування за безумовними критеріями.

В табл. 3 представлені показники швидкості процедур встановлення ключа, встановлення мітки часу, процедури генерації ключового потоку та зашифровування 40-байтного пакету в тактах процесора, які були взяті із [1] для процесора Intel Core 2 Quad Q6600 6fb, amd64 architecture.

Таблиця 3

Назва шифру	Встановлення ключа, встановлення мітки часу, генерація ключового потоку та зашифровування	Місце	$K_{б6}$
Rabbit	28	4	1
Salsa20	17	2	1
Sosemanuk	41	6	1
HC-128	500	8	0
NLS v2	37	5	1
LEX v2	20	3	1
CryptMT v3	15	1	1
Dragon	52	7	1

Як вже відмічалося, шифри, що є найгіршими по швидкості, отримують $K_{б6} = 0$. Для інших – $K_{б6} = 1$.

Підсумкові значення показників $K_{б1} - K_{б6}$ наведені у табл. 4.

Таблиця 4

Назва шифру	$K_{б1}$	$K_{б2}$	$K_{б3}$	$K_{б4}$	$K_{б5}$	$K_{б6}$
Rabbit	1	1	1	1	1	1
Salsa20	1	1	1	1	1	1
Sosemanuk	1	1	1	1	1	1
HC-128	1	1	1	1	1	0
NLS v2	0	1	1	1	1	1
LEX v2	0	1	1	1	1	1
CryptMT v3	0	1	1	1	1	1
Dragon	0	1	1	1	1	1

З цієї таблиці видно, що розглядати умовні критерії варто лише для шифрів Rabbit, Salsa20 та Sosemanuk.

4.2 Порівняльний аналіз алгоритмів шифрування за умовними критеріями.

Першим умовним критерієм є частковий критерій оцінки можливість та умови поширення алгоритму шифрування. По цьому критерію пропонується оцінювати:

– умови розробки та дослідження (наявність) обмежень уже на цьому етапі;

– відсутність обмежень на експорт;

– відсутність обмежень на імпорт;

– необхідність одержання ліцензії на використання алгоритму;

– контроль за застосуванням та обов'язковість звітування;

– наявність обмежень на експорт засобів, що реалізують алгоритм;

– наявність патентів на алгоритм та його складові.

Значення цих показників визначені на основі вивчення нормативно-правових актів, що діють на міжнародному і національному рівнях.

На основі описаних вище показників методом експертних оцінок установлюються переваги того або іншого претендента у вигляді вагових коефіцієнтів приватного критерію

$$K_{y1} = \sum W_i,$$

де W_i – числові значення усереднених експертних оцінок (вагового коефіцієнта) для кожного з варіантів.

Варто помітити, що алгоритми Rabbit, Salsa20 та Sosemanuk є відкритими для некомерційного використання.

У табл. 5 наведені результати оцінки по приватному умовному критерію поширення алгоритму. Усього за цим критерієм будемо використовувати 7 показників W_i, що наведені вище. Кожний з показників може приймати три значення:

0 – є обмеження;

1 – не визначений;

2 – дозволений або не обмежений.

Таблиця 5

Показники / Алгоритми	W_1	W_2	W_3	W_4	W_5	W_6	W_7	K_{y1}
Rabbit	2	1	1	1	1	1	1	8
Salsa20	2	1	1	1	1	1	1	8
Sosemanuk	2	1	1	1	1	1	1	8

Критерій рівня довіри алгоритмові шифрування будемо визначати по складеним W_{21}, W_{22}, W_{23} (усереднені експертні оцінки) третього приватного умовного критерію K_{y2}:

$$K_{y2} = W_{21} + W_{22} + W_{23},$$

де W_{21} – оцінка ступеня відкритості правил проектування і прозорості використовуваних методів; W_{22} – достатність кількості і авторитет числа незалежних дослідників, що аналізують стійкість і властивості шифру; W_{23} – оцінка відсутності підозр на наявність вразливостей.

У табл. 6 наведені значення показника K_{y2} і його складових W_{21}, W_{22} і W_{23}. Оцінка зроблена як і вище по трьохбальній системі $W_{3i} \in \{0, 1, 2\}$.

Таблиця 6

Показники / Алгоритми	W_{21}	W_{22}	W_{23}	K_{y2}
Rabbit	1	1	1	3
Salsa20	1	1	1	3
Sosemanuk	1	1	1	3

Оцінка перспективності застосування алгоритму шифрування зроблена використовуючи приватний умовний критерій K_{y3} і відповідні показники W_{3i}:

$$K_{y3} = W_{31} + W_{32} + W_{33} + W_{34},$$

де W_{31} – числове значення (вага) експертної оцінки про перевагу шифру на основі зведень про його використання в якості міжнародного стандарту (стандартів) і/або національного стандарту (стандартів); W_{32} – числове значення експертної оцінки показника ступеня поширеності алгоритму; W_{33} – числове значення експертної оцінки існування (відсутності) підозр на теоретичну можливість здійснення криптоаналітичної атаки і її погрози; W_{34} – числове значення експертної оцінки можливості застосування в перспективних інформаційних технологіях.

Оцінка зроблена по трьохбальній системі показників.

У табл. 7 наведені значення показників і приватного критерію K_{y3}.

Таблиця 7

Показники / Алгоритми	W_{31}	W_{32}	W_{33}	W_{34}	K_{y3}
Rabbit	1	1	1	1	4
Salsa20	1	1	1	1	4
Sosemanuk	1	1	1	1	4

Оцінка тимчасової і просторової складності, програмної, апаратної й апаратно-програмної реалізацій прямого і зворотного перетворень виконана з використанням приватного критерію K_{y4}:

$$K_{y4} = W_{41} + W_{42} + W_{43} + W_{44},$$

де W_{41} – числове значення експертної оцінки показника складності прямого криптографічного перетворення; W_{42} – числове значення експертної оцінки показника складності зворотного криптографічного перетворення; W_{43} – числове значення експертної оцінки просторової складності; W_{44} – числове значення експертної оцінки розміру вихідного коду реалізації (реалізацій). При оцінці використовувалися результати досліджень, що наведені в розділі 4.1. Результати оцінки наведені в табл. 8. Оцінка виконана по трьохбальній системі.

Таблиця 8

Показники / Алгоритми	W_{41}	W_{42}	W_{43}	W_{44}	K_{y4}
Rabbit	1	1	1	1	4
Salsa20	2	2	1	1	6
Sosemanuk	0	0	1	1	2

Аналіз показника K_{y4} показує, що алгоритми шифрування по цьому показнику розміщені в такій послідовності Rabbit, Salsa20 і Sosemanuk.

Оцінка ступеня гнучкості здійснювалася згідно критерію K_{y5}:

$$K_{y5} = W_{51} + W_{52} + W_{53} + W_{54}, + W_{55},$$

де W_{51} – числове значення експертної оцінки можливості зміни довжини ключа; W_{52} – числове значення експертної оцінки можливості реалізації на різних програмних платформах; W_{53} – числове значення експертної оцінки можливості апаратної реалізації; W_{54} – можливість використання для реалізації криптографічних протоколів.

Результати оцінки зведені в табл. 9.

Таблиця 9

Показники / Алгоритми	W_{51}	W_{52}	W_{53}	W_{54}	K_{y5}
Rabbit	0	2	2	2	6
Salsa20	2	2	2	2	8
Sosemanuk	1	2	2	2	7

З табл. 9 випливає, що алгоритми шифрування по цьому показнику розміщені в такій послідовності Salsa20, Sosemanuk і Rabbit.

Тепер методом експертної оцінки для кожного з розглянутих алгоритмів шифрування для кожного критерію визначаємо нечіткі множини:

$$\mu_{K_{y1}} = \{1/8 + 0{,}7/8 + 0{,}6/8\};$$

$$\mu_{K_{y2}} = \{0{,}8/3 + 0{,}6/3 + 0{,}5/3\};$$

$$\mu_{K_{y3}} = \{0{,}7/4 + 0{,}5/4 + 0{,}3/4\};$$

$$\mu_{K_{y4}} = \{0{,}9/4 + 0{,}8/6 + 0{,}8/2\};$$

$$\mu_{K_{y5}} = \{0{,}5/6 + 0{,}5/8 + 0{,}4/7\}.$$

Цей запис розуміється так: для кожного часткового умовного критерію отримані значення $K_{y1} - K_{y5}$ – (табл. 5 – 9) перетворяться в нечіткі множини за допомогою згортки (2).

У нашому випадку всі часткові умовні критерії $K_{y1} - K_{y5}$ мають різну значимість при виборі найбільш кращого варіанту. У зв'язку з цим необхідно визначити вагові коефіцієнти β_i цих критеріїв. Один з можливих способів одержання значень вагових коефіцієнтів полягає в побудові матриці попарних порівнянь критеріїв. Для приватних умовних критеріїв маємо відповідну таблицю.

Таблиця 10

Умовні критерії	K_{y1}	K_{y2}	K_{y3}	K_{y4}	K_{y5}
K_{y1}	1	1	3	1/3	3
K_{y2}	1	1	3	1/5	3
K_{y3}	1/3	1/3	1	1/5	3
K_{y4}	3	5	5	1	3
K_{y5}	1/3	3	1/3	1/3	1

Ваговий коефіцієнт критеріїв β_i визначається на підставі обчислених значень правого часткового вектора матриці попарних порівнянь α_i з наступним множенням на число критеріїв n:

$$\beta_i = \alpha_i n.$$

Значення α_i і β_i наведені в табл. 11.

Таблиця 11

Власний вектор матриці попарних порівнянь критеріїв і їх вагові коефіцієнти

	K_{y1}	K_{y2}	K_{y3}	K_{y4}	K_{y5}
Значення α_i	0,19	0,172	0,089	0,451	0,098
Значення β_i	0,95	0,86	0,445	2,255	0,49

Множина оптимальних альтернатив D з урахуванням різної важливості критеріїв ефективності визначається шляхом перетинання нечітких множин згідно (2).

Знайдемо множину оптимальних альтернатив з обліком отриманих вагових критеріїв по формулі (2):

$D = \{ \min \{ 1{,}0^{0{,}95}; 0{,}8^{0{,}86}; 0{,}7^{0{,}445}; 0{,}9^{2{,}255}; 0{,}5^{0{,}49}\}$,
$\min \{ 0{,}7^{0{,}95}; 0{,}6^{0{,}86}; 0{,}5^{0{,}445}; 0{,}8^{2{,}255}; 0{,}5^{0{,}49}\}$,
$\min \{ 0{,}6^{0{,}95}; 0{,}5^{0{,}86}; 0{,}3^{0{,}445}; 0{,}8^{2{,}255}; 0{,}4^{0{,}49}\}\}$.

Згортка множини оптимальних варіантів для алгоритмів Rabbit, Salsa20 і Sosemanuk відповідно має вигляд:

1. По методу мінімуму:

$$\max_j \mu_D(a_j) = \max\{0{,}712; 0{,}217; 0{,}585\}.$$

2. З урахуванням зваженої оцінки всіх критеріїв:

$$\max_j \mu_D(a_j) = \max\{0{,}358; 0{,}035; 0{,}066\}.$$

Таким чином, запропонована методика дозволяє здійснити порівняльний аналіз перспективних алгоритмів шифрування.

У табл. 12 наведені значення безумовного й умовного критерію оцінки алгоритмів шифрування.

Таблиця 12

Результати порівняльного аналізу перспективних ПСШ

Критерії / Алгоритми		Rabbit	Salsa20	Sosemanuk
Безумовний $K_б$		1	1	1
Умовний $K_у$	Метод мінімуму	0,712	0,605	0,585
	Облік усіх критеріїв	0,395	0,145	0,077

Аналіз даних табл. 12 дозволяє зробити висновок, що найбільш кращим є алгоритм Rabbit. На другому місці знаходиться алгоритм ПСШ Salsa20, на третьому – Sosemanuk. Тому, на наш погляд, можна зробити висновок про те, що в Україні для вирішення задач забезпечення конфіденційності інформації сьогодні доцільно рекомендувати до використання алгоритм потокового симетричного шифрування Rabbit.

Rabbit є однією з найстаріших конструкцій проекту eSTREAM. Даний потоковий симетричний шифр не був підданий яким-небудь модифікаціям або доповненням. Його специфікація залишалася незмінної з 2003 року й по даний момент. Шифр пережив усі три етапи проекту й не на одному з них не був підданий криптоаналітичним атакам. Крім

усього іншого даний алгоритм дуже добре реалізується на нових процесорах сімейства Intel.

Література.

[1] *Горбенко І.Д., Гулак Г.М., Олійников Р.В., Руженцев В.І., Михаленко М.С.* Аналіз властивостей алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE). //Радіотехніка, 2005 №141.

[2] *Горбенко І.Д., Пушкарьов А.І., Олійников Р.В., Руженцев В.І., Горбенко Ю.І., Михайленко М.С.* Порівняльний аналіз алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE). //Радіотехніка, 2005 №141.

[3] *Daniel J. Bernstein,* «Which phase-3 eSTREAM ciphers provide the best software speeds?» Доклад з проекту eSTREAM 2008/013 (оновлений 31.03.2008) URL: http://www.ecrypt.eu.org/stream/papers.html.

[4] *Daniel J. Bernstein,* «Which eSTREAM ciphers have been broken?» Доклад з проекту eSTREAM 2008/010 (оновлений 30.03.2008) URL: http://www.ecrypt.eu.org/stream/papers.html.

Надійшла до редколегії 17.09.2008

Горбенко Іван Дмитрович, професор, зав. кафедрою БІТ ХНУРЕ, головний конструктор ЗАТ «ІІТ». Область наукових інтересів: проектування та розробка засобів КЗІ.

Нейванов Андрій Вікторович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: симетрична криптографія, програмування, теорія ймовірності та математична статистика.