DOI: 10.35681/1560-9189.2021.23.1.235158

УДК 004.056.55

А. В. Волошко, Т. М. Лутчин
Інститут енергозбереження та енергоменеджменту
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
вул. Борщагівська, 115, 03056 Київ, Україна
тел. 050 221 0132, e-mail: avolosko820@gmail.com

Комбінований метод шифрування даних з ідентифікацією їхнього відправника

На основі аналізу узагальнених моделей інформаційних потоків на основі часово-просторових властивостей вейвлет-коефіцієнтів за рівнями вейвлет-декомпозиції запропоновано узагальнений метод шифрування даних із можливістю ідентифікації відправника повідомлення. Закритий ключ шифрування — пароль, що складається з чотирьох складових, його довжина — 324 біта. Розшифрування потребує орієнтовно 10^{12} операцій та обов'язкового знання вибраного вейвлет-базису над модифікованими даними (вейвлет-коефіцієнтами інформаційних даних із закодованим ключем). До зашифрованого повідомлення застосовується зворотне вейвлет-перетворення, коефіцієнти якого і будуть передаватися лініями зв'язку у вигляді відкритого ключа. Несанкціонований вплив на дані, які передаються, повністю виключається завдяки часово-просторовим і спектральним властивостям вейвлет-коефіцієнтів за рівнями вейвлет-декомпозиції. Відносна похибка оберненого вейвлет-перетворення знаходиться в межах від $4 \cdot 10^{-14}$ до $6 \cdot 10^{-14}$.

Ключові слова: *шифрування, вейвлет-аналіз, закритий ключ.*

Вступ

Процес впровадження нових інформаційних технологій, розгалужених інформаційно-обчислювальних систем у всі сфери життєдіяльності немислимий без вирішення питань інформаційної безпеки. Що стосується електроенергетики у цьому плані, то необхідно відмітити, що всі учасники ринку електроенергетики України (від генерації електричної енергії, транспортування, розподілення і до її споживання) об'єднані в розгалужені інформаційні системи, інформація в яких носить комерційний (закритий) характер. Також немаловажним у плані безпеки інформації є те, що з реформуванням електроенергетичного господарства України

(впровадженням Smart Grid-технологій) буде спостерігатися підключення великої кількості постачальників/споживачів електричної енергії до локальних і розподілених комп'ютерних мереж учасників енергоринку, а отже і до серверних ресурсів, що виводить питання уникнення несанкціонованого доступу до інформації (включаючи бази даних, лінії зв'язку) на перше місце.

Аналіз наукових публікацій

Одними із самих ефективних методів захисту інформації від несанкціонованого доступу при їхній передачі відкритими каналами зв'язку та зберіганні є кодування та шифрування. З теоретичної точки зору не існує чіткої різниці між кодами та шифрами. Однак у сучасній практиці відмінність між ними, як правило, є достатньо чіткою. Коди оперують лінгвістичними елементами, поділяючи текст, що шифрується, на смислові елементи — слова та склади. У шифрі завжди розрізняють два елементи — алгоритм і ключ.

Криптосистеми поділяються на симетричні та асиметричні. Симетрична криптосистема (симетричне шифрування) — спосіб шифрування, в якому для шифрування та розшифрування застосовується один і той же самий ключ, який повинен зберігатись у таємниці двома сторонами. Основними симетричними криптографічними алгоритмами є: поодинока та подвійна перестановка по ключу; перестановка «магічний квадрат» та проста перестановка; блочні шифри Гронфельда, Бофора, Віжінера і т.п. [1].

Найбільш відомими та більш криптостійкими алгоритмами симетричних шифрів є: AES (Advanced Encryption Standard) та DES (Data Encryption Standard) — стандарти шифрування США [2]; IDEA (International Data Encryption Algorithm) — інтернаціональний; SEAL (Software Efficient Algorithm) — ефективний програмний; WAKE (World Auto Key Algorithm) — всесвітній алгоритм шифрування на автоматичному ключі [3]; ГОСТ 28147-89 — російський стандарт [4].

Аналіз найбільш поширених алгоритмів шифрування показав наступне. В першу чергу це алгоритм DES, який представляє собою типовий симетричний блочний шифр і використовує ключі довжиною в 256 біт. Застосовується для передачі даних у мережі «всі-до-всіх» і перетворює відкритий текст, який представляється у вигляді послідовності бітів (нулів та одиниць), на блоки фіксованої тривалості (довжини), частіше всього рівної 64 біт або 128 біт. Секретний ключ також представляється послідовністю біт (128–256), з якого, за визначеним для кожного шрифту механізмом, отримується набір із R-послідовностей [5].

Починаючи з 1997 року, приймалося багато спроб збільшити його криптостійкість шляхом оптимізації процесу проведення раундів (послідовностей) [6], але на об'явленому NIST конкурсі (серед претендентів були стандарти CRYPTREC [7] — Японія, NESSIE — Європа, MARS [8]) перемогу, як національний, отримав шифр RISNDAEL [9].

Алгоритм шифрування, який представлений у ГОСТ 28147, має всі переваги алгоритму DES, але при цьому він має і істотний недолік, який полягає в тому, що його програмна реалізація дуже складна і практично позбавлена всякого сенсу із-за вкрай низької швидкодії. У табл. 1 та табл. 2 наведено час розшифрування та довжина ключа для різних алгоритмів відповідно.

Як слідує з табл. 1, 2, довжина ключа є досить важливим чинником, який суттєво впливає на криптостійкість шифру.

Таблиця 1. Довжина ключа/час розшифрування

Довжина ключа, біт	Час розшифрування
10	<1 сек.
20	21 сек.
30	6 годин
40	255 днів
64	>12 років
128	>200 років

Таблиця 2. Довжина ключа/тип алгоритму

Тип алгоритму	Довжина ключа, біт
DES	56
IDEA	128
AES	змінна
WAKE	
SEAL	
ГОСТ 28147	

Підсумовуючи проведений аналіз застосування алгоритмів симетричних криптосистем, необхідно відмітити наступне. По-перше, алгоритми, які використовують різного роду підстановки, перестановки та гамування є самими простими та застосовуються переважно для шифрування текстової інформації. Основним їхнім недоліком є невелика швидкість шифрування — при їхньому виконанні використовується велика кількість проходів (раундів), для яких застосовується свій «ключ проходу». Чим більша кількість проходів, тим вища криптостійкість, але при цьому різко зменшується швидкість шифрування.

По-друге, нарівні зі своїми перевагами над асиметричними алгоритмами (швидкість на 3 порядки вище, реалізація потребує більш простих операцій, менша довжина ключа за однакової криптостійкості) вони мають суттєвий недолік — складність управління ключами у великій мережі (для мережі із 10 абонентів необхідно згенерувати 45 ключів, а для мережі зі 100 абонентів — 4950 і т.д.) та складність обміну ключами, що дуже впливає на їхню криптостійкість.

По-третє, при застосуванні симетричних алгоритмів неможливе їхнє використання для цифрового підпису, оскільки ключ відомий кожній зі сторін.

Асиметричні криптосистеми є ефективними криптографічними системами захисту даних, які ще носять назву криптосистем з відкритим ключем. У таких системах для шифрування даних використовується один ключ, а для розшифрування — інший. Перший ключ є відкритим і може бути опублікованим для використання всіма користувачами системи, які шифрують дані. Розшифрування даних за допомогою відкритого ключа неможливе. Для цього використовується другий ключ, який є секретним.

Початок розробкам асиметричних шифрів було покладено в роботі Уітфілда Діффі та Мартіна Хеллмана, яка була опублікована в 1976 році. В ній вони запропонували метод отримання секретних ключів, використовуючи відкритий канал. У 1995 році вчений R.L. Rivest [10] запропонував ефективний алгоритм шифрування даних (RC5), який був модифікований у 1977 році вченими Р. Ріверстом (Ronald Linn Rivest), А. Шаміром (Adi Shamir) та Л. Адлеманом (Leonard Adleman), і називається RSA [11]. Алгоритм RSA став першим алгоритмом, придатним як для шифрування, так і для цифрового підпису. У подальшому цей напрям шифрування отримав назву — криптографія з відкритим ключем — асиметрична схема, в якій застосовується пара ключів: відкритий (public key), що зашиф-

ровує дані, і відповідний йому закритий (private key), що їх розшифровує. У зв'язку з тим, що обидва ключі (відкритий і закритий) є математично пов'язані, можливе дешифрування даних сторонніми користувачами.

Так, у 2004 р. учений L. Harn запропонував три різних протоколи передачі закритого ключа та використовувати алгоритм RSA не тільки для шифрування даних, а і для використання цифрового підпису [12]. Такі алгоритми отримали загальну назву — DSA (Digital Signature Algorithm) Diffie-Hellmana. Незважаючи на наявність недоліків асиметричних алгоритмів по відношенню до симетричних, вони є більш комплексними у застосуванні. Їх можна використовувати як: самостійний засіб захисту даних, які передаються та зберігаються; засіб для розподілення ключів (спочатку передача ключа, потім зашифрованих даних); засіб аутенфікації користувача (подібно до електронному підпису).

Аналіз переваг і недоліків існуючих алгоритмів дозволив сформулювати загальні вимоги до алгоритму шифрування, а саме:

1) поява потужних комп'ютерів, технологій мережевих і нейронних обчислень зробили можливим дискредитацію криптографічних схем, які ще недавно вважалися такими, що не дешифруються. Виходячи з цього, необхідно разом із застосуванням ключів шифрування, впроваджувати в алгоритми шифрування допоміжні математичні методи, які підвищать криптостійкість шифрів;

2) знання алгоритму шифрування не повинно впливати на криптографічну стійкість;

3) незначні зміни ключа повинні приводити до суттєвих змін повідомлень, які захищаються, навіть у випадку використання одного й того ж ключа;

4) структурні елементи алгоритму шифрування повинні бути незмінні;

5) не повинно бути простих і легко встановлюваних залежностей між ключами, які використовуються в процесі шифрування;

6) алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна приводити до якісного погіршення алгоритму шифрування;

7) алгоритм повинен допускати аутенфікацію відправника повідомлення і мати можливість виявляти спроби зміни повідомлення (несанкціонованого доступу).

Підсумовуючи вимоги до алгоритму шифрування бачимо, що ні один відомий алгоритм окремо їм не відповідає. Тобто, необхідно на рівні з компенсацією недоліків симетричних систем, використанням переваг асиметричних, застосувати математичні методи трансформування і самого алгоритму шифрування для підвищення криптографічної стійкості.

Враховуючи той факт, що в роботі представлені узагальнені моделі інформаційних потоків на основі часово-просторових властивостей ортогональних перетворень, доцільно на основі даних моделей розробити узагальнений алгоритм шифрування з обов'язковою можливістю ідентифікації відправника повідомлення.

Розробка комбінованого методу шифрування даних з ідентифікацією їхнього відправника

Як відомо, шифром називається пара алгоритмів, які реалізують шифрування та розшифрування даних. При цьому необхідно відмітити декілька обмежень:

— шифр повинен бути криптостійким. При цьому міра невизначеності повідомлення визначається:

$H(T) = -\sum_{i=1}^{n} P_i \log_2 P_i$ — апріорно, а $H(T/\hat{T}) = -\sum_{i=1}^{n} P(T/\hat{T}) \log_2 P_i(T/\hat{T})$ — апостеріорно;

— кількість інформації про вихідне повідомлення:

$$J = H(T) - H(T/\hat{T}),$$

де T — вихідне повідомлення; $\hat{T}$ — зашифроване повідомлення.

При цьому найкращий шифр, це коли $H(T/\hat{T}) = H(T)$, при $J = 0$ — стійкий шифр, тобто повинно виконуватися наступне: $\hat{T} = E(T) = E_k(T)$, де k — ключ шифру; $E(\bullet)$ — функція (процедура) шифрування; $D(\hat{T}) = T$ — функція (процедура) розшифрування.

Враховуючи дані обмеження, результати порівняльного аналізу відомих алгоритмів шифрування і враховуючи той факт, що в роботі представлені узагальнені моделі інформаційних потоків на основі часово-просторових властивостей вейвлет-коефіцієнтів за рівнями вейвлет-декомпозиції, доцільно на основі даних моделей розробити узагальнений метод шифрування з обов'язковою можливістю ідентифікації відправника повідомлення.

Розроблений авторами комбінований асиметричний метод шифрування інформаційних даних з ідентифікацією відправника базується на властивостях пакетного вейвлет-перетворення і сучасних методах шифрування.

Пакетне вейвлет-перетворення представляє собою рекурсивне розщеплення векторів просторів, які формують структуру бінарного дерева, яке складається з 2^j параметрів вейвлет-коефіцієнтів на всіх рівнях перетворення. Пакетне вейвлет-перетворення є адаптивним, що не потребує навчання або відомостей про статистичні властивості інформаційних сигналів і дозволяє більш точно враховувати особливості сигналу. що аналізується, шляхом вибору відповідної оптимальної форми дерева та розкладу.

Вейвлет-пакети були введені Куафманом, Мейером і Вікерхаузером [13] як узагальнення зв'язуючої ланки між кратномасштабними апроксимаціями та вейвлетами. Простір V_j кратномасштабної апроксимації розкладається на суму просторів більш низького розподілу V_{j+1} та простору подробиць W_{j+1}. Це здійснюється розбиттям ортогонального базису $\left\{\varphi_{j+1}(t-2^{j+1}n)\right\}_{n\in\mathbb{Z}}$ простору V_{j+1} та $\left\{\psi_{j+1}(t-2^{j+1}n)\right\}_{n\in\mathbb{Z}}$ простору W_{j+1}. Функція ψ — материнський вейвлет з нульовим середнім значенням $\int_{-\infty}^{+\infty} \psi(t)dt = 0$ і параметрами розтягнення s та параметром зсуву u:

$$\psi_{u,s}(t) = \frac{1}{\sqrt{s}}\psi\left(\frac{t-u}{s}\right), \tag{1}$$

розтягнення та зсув якої породжують ортонормований базис у $L^2(\mathbb{R})$:

$$\left\{\psi_{j,n}(t) = \frac{1}{\sqrt{2^j}}\psi\left(\frac{t-2^j n}{2^j}\right)\right\}_{(j,n)\in\mathbb{Z}^2}. \tag{2}$$

Інформаційний сигнал $f(t)$ може бути відновлений на j-му рівні розкладу за своїм дискретним вейвлет-спектром за допомогою співвідношення

$$f(t) = \sum_{k=-\infty}^{\infty} a_{j_n,k}\varphi_{j_n,k}(t) + \sum_{j=j_n}^{\infty}\sum_{k=-\infty}^{\infty} d_{j,k}\psi_k(t), \tag{3}$$

де $a_{j,k} = \int_{-\infty}^{\infty} f(t)\psi_{j,k}(t)dt$ — апроксимуючі вейвлет-коефіцієнти;

$\varphi_{j,k}(t) = 2^{j/2}\varphi(2^j t - k)$ — скейлінг-функція;

$d_{j,k}$ — деталізуючі коефіцієнти.

Реальний інформаційний сигнал $f(t)$ завжди задається кінцевою кількістю точок N. Тому і максимальне число рівнів розкладу $J_{\max}$ ($J_{\max} \in \mathbb{N}, \mathbb{N}$ — множина натуральних чисел) також є обмеженим. Воно визначається співвідношенням $J_{\max} \le \log_2 \mathbb{N}$. Враховуючи, що наш інформаційний сигнал представляє собою графік електричного навантаження (ГЕН), за ортонормований базис вибираємо вейвлет Хаара:

$$\varphi(t) = rect(t - 1/2), \text{ де } rect(t-1/2) \equiv 1 \text{ при } t \in [0,1],$$

$$\psi(t) = rect[2(t-1)] - rect[2(t-3/4)],\ \hat{\psi}(\omega) = 4j\left[\frac{1-\cos(\omega/2)}{\omega}\right]e^{-j\omega/2}. \tag{4}$$

Запропонований метод шифрування та ідентифікації відправника складається із наступних етапів [14].

Етап 1. Після попередньої обробки інформаційних даних шляхом їхнього усереднення ($\hat{Y}_i = Y_i / \bar{Y}_c$, де $\bar{Y}_c$ — середнє значення часового ряду, Y_i — поточне значення ряду), виконується пакетне вейвлет-перетворення, рівень якого обирається із властивостей вейвлет-аналізу. Відносно ГЕН — то це є п'ятий рівень. Виходячи з характеристики ряду (ГЕН), як базис розкладання застосовується вейвлет Хаара (4). В результаті отримується частотно-впорядкований ряд із 32 вейвлет-коефіцієнтів $\{k_{5,i}\}_{0\le i\le 31}$.

Етап 2. Проводиться формування закритого ключа шифру — пароля. Згідно з властивостями вейвлет-коефіцієнтів (наявністю їхніх функціональних зв'язків за

рівнями вейвлет-декомпозиції) з отриманого ряду випадковим чином відкидаємо вейвлет-коефіцієнти в межах основного набору $\{k_{5,4s}, k_{5,4s+1}, k_{5,4s+2}, k_{5,4s+3}\}$, де $s \in [1;8]$ — згруповані вейвлет-коефіцієнти відповідно до функціональних зв'язків. Замість відкинутого вейвлет-коефіцієнта у вибірку тимчасово записується нульове значення. Позиція нульового значення вейвлет-коефіцієнта являє собою першу складову закритого ключа *r*. З метою підвищення стійкості закритого ключа шифрування замість нульового значення підставляємо випадковим чином згенероване середнє значення початкового ряду $P_{c,зг} = P_c$ (0,75 + 0,5 RND), де RND — генератор випадкових чисел. На даному етапі формується друга складова закритого ключа — *d* ($P_{c.зг}$).

Для подальшого підвищення стійкості закритого ключа в даному алгоритмі застосовується збільшення вихідного значення шляхом додавання на порядки більшу величину *a*. Потім вихідна вибірка підноситься в довільну ступінь *b*. У загальному вигляді маємо $P_n = (P_c + a)^b$, де *a* і *b* являються третьою та четвертою складовими закритого ключа відповідно. В результаті сформовано закритий ключ — *r*, *d*, *a*, *b*. Довжина закритого ключа складає 324 біта. Його розшифрування потребує орієнтовно 10^{12} операцій та обов'язкового знання обраного базису.

Етап 3. Над модифікованими даними (вейвлет-коефіцієнтами) проводиться зворотне вейвлет-перетворення [15], коефіцієнти якого і будуть передаватися лініями зв'язку у вигляді відкритого ключа.

Перевірку запропонованого методу шифрування здійснено на прикладі даних щодо навантаження енергосистеми та електричних станцій України в режимний день 2016 р. Доведено, що точність дешифрування вихідних значень ГЕН визначається виключно точністю використаного програмного забезпечення; відносна похибка, обумовлена вейвлет-перетворенням, складає $\sim 10^{-13}$.

Таким чином, запропонований комбінований метод на основі властивостей вейвлет-перетворення та передових методів шифрування наряду з процесом шифрування дозволяє повністю ідентифікувати відправника. Для додаткового підвищення стійкості закритого ключа шифрування, при проведенні зворотного вейвлет-перетворення, може застосовуватися неповне вейвлет-перетворення. У випадку несанкціонованого відновлення даних відбудеться хибне нарощування вейвлет-коефіцієнтів вибірки $\{P_{c.сг}, k_{5,4s+1}, k_{5,4s+2}, k_{5,4s+3}\}$. При цьому задається додаткова складова закритого ключа.

Параметри *a* та *b* обираються залежно від пропускної здатності каналів зв'язку. Великі значення даних параметрів призведуть до перевантаження каналів зв'язку, не підвищуючи стійкості закритого ключа шифрування. Подальше підвищення стійкості закритого ключа можливе шляхом використання властивостей взаємозв'язків між вейвлет-коефіцієнтами, випадковим чином відкинувши будь-який з них.

Несанкціонований вплив на дані, які передаються, повністю виключається завдяки частотно-просторовим і спектральним властивостям вейвлет-коефіцієнтів за рівнями вейвлет-декомпозиції. Відносна похибка оберненого вейвлет-перетворення знаходиться в межах від $4 \cdot 10^{-14}$ до $6 \cdot 10^{-14}$.

Практична реалізація методу шифрування та аналіз похибки зворотного дешифрування

Як практичне застосування розробленого комбінованого методу шифрування даних розглянуто реальні графіки навантаження енергосистеми, електричних станцій, включаючи навантаження ТЕЦ, ГЕС і блок-станцій у режимний літній день 2016 року.

Як було відмічено раніше, в результаті вейвлет-перетворення вхідних даних, які приведені до середнього значення, формується вибірка даних (етап 2). Для подальшого кроку приймається число $r = 2$ (тобто, відкидається кожний другий елемент вибірки $\{k_{5,4s}, k_{5,4s+1}, k_{5,4s+2}, k_{5,4s+3}\}$).

Потім генеруються випадковим чином середні значення (табл. 3).

Таблиця 3. Дійсні та згенеровані середні значення досліджуваних вибірок

	1	2	3	4	5	6
P_c	20877,9	20437,33	9967,79	868,67	9600,88	440,58
$P_{c,g1}$	33790,3	28559,88	18957,2	1394,55	17653,17	20,1309
$P_{c,g2}$	29548,6	151,6989	5326,96	1596,14	1793,195	344,351
$P_{c,g3}$	25151	38844,4	19737,7	36,7237	8838,201	770,32
$P_{c,g4}$	38878,5	27163,76	17599,6	1072,74	12430,59	877,406
$P_{c,g5}$	37623,7	15210,29	17818,6	1582,19	2489,38	251,535
$P_{c,g6}$	37919,2	8665,169	313,767	284,215	4521,687	736,229
$P_{c,g7}$	20019,2	26757,13	497,787	274,734	16516,09	64,4046

g — індекс, яким відмічено згенеровані значення.

На наступному етапі проводиться перетворення вибірок з урахуванням значень $a = 121000$ та $b = 5$. Потім для підняття ступеню захисту вдруге проводиться вейвлет-перетворення (рис. 1).

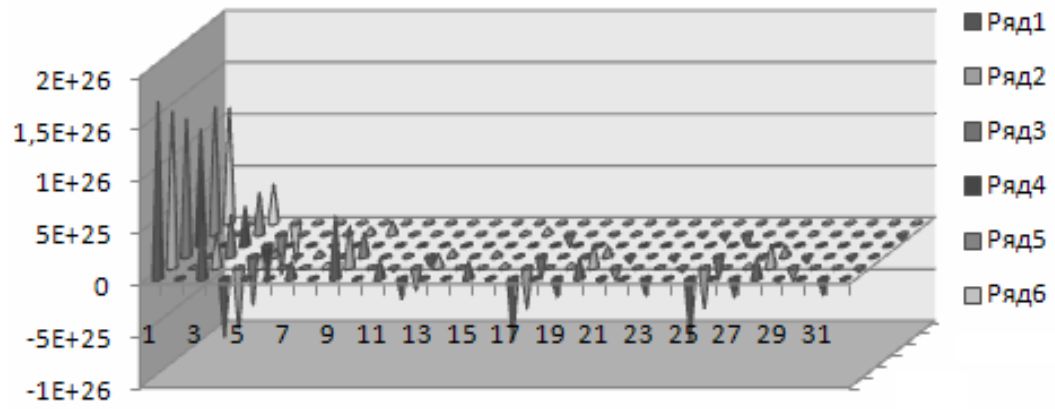

Рис. 1. Ряди коефіцієнтів повторного вейвлет-перетворення

Результатом такого шифрування є відкритий ключ — значення вейвлет-коефіцієнтів і закритий шифр 261210005 ($r = 2$, $s = 6$, $a = 121\,000$, $b = 5$). У результаті відновлення вихідних значень ГЕН похибка дешифрування визначається тільки форматом представлення чисел у використовуваному програмному забезпеченні. У даному випадку числові результати представлені у нормалізованій формі з чотирма знаками після десятинної коми і одним до неї. Значення похибки, яку вносить зворотне вейвлет-перетворення, представлене на рис. 2.

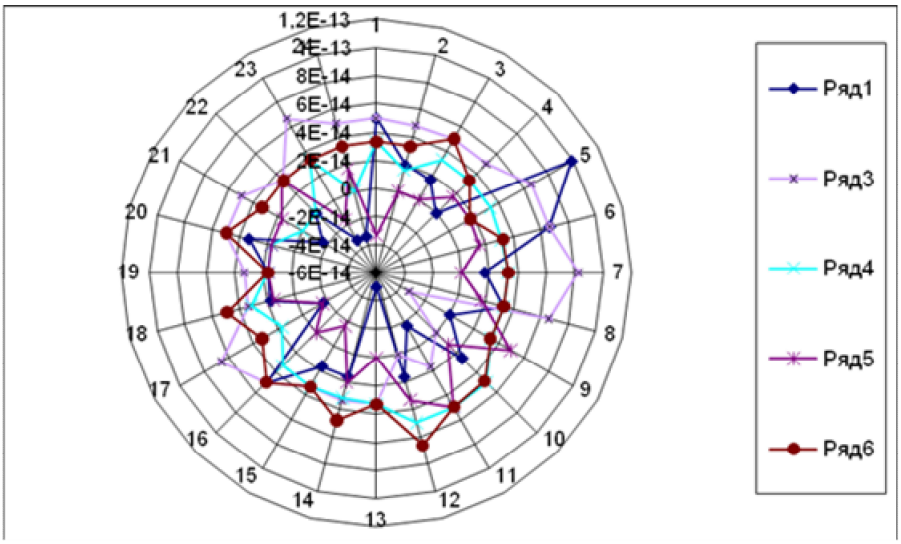

Рис. 2. Значення відносної похибки при зворотному вейвлет-перетворенні

Висновки

1. У запропонованому методі шифрування перші дві складові — завжди натуральні числа від 0 до 10. Для зручності користування шифром пропонується параметр a задавати випадковим натуральним числом, а параметр b — натуральним числом від 0 до 10, або параметр $a \geq 4{,}234$, а параметр b — дійсним числом. При цьому слід зауважити, що невиправдано великі значення даних параметрів можуть призвести до перевантаження ліній зв'язку, при тому, що точність шифрування не підвищиться.

2. Для збільшення надійності шифрування необхідно використовувати таку властивість вейвлет-коефіцієнтів як взаємозалежність (на основі аналізу функціональних зв'язків) $\left\{k_{5,4s}, k_{5,4s+1}, k_{5,4s+2}, k_{5,4s+3}\right\}$, тобто, знехтувати деяким довільним коефіцієнтом, а потім проводити шифрування даних згідно до вищенаведеного методу.

3. На основі розробленого методу шифрування пропонується спосіб обміну даних в енергосистемі. Він полягає в наступному. На стороні об'єкта, який спостерігається, встановлюється модуль прямого вейвлет-перетворення з можливістю задавання алгоритму шифрування. На стороні управління — модуль зворотного вейвлет-перевторення та база зберігання індивідуальних шифрів по кожному з

об’єктів управління, які і являються засобом ідентифікації відправника повідомлення.

1. Берников В.О. Сравнительный анализ криптостойкости симметричных алгоритмов шифрования. Труды БПТУ. Сер 3. Физико-математические науки и информатика. Минск: БГТУ. 2020. № 1. С. 74–78.

2. Горбенко Ю.І., Мордвінов Р.І., Кузнецов О.О. Розробка математичних та програмних модулей перспективного алгоритму шифрування для перевірки правильності реалізації. *Восточно-Европейский журнал передовых технологий*. 2014. **5/9(**71). С. 21–29.

3. Kapalova N., Khompysh A., Algazy K. A block encryption algorithm based on exponentiation transform. *Cogent Engineering*. 2020. Vol. 7. Issue. 1. P. 211–219.

4. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Текст]: ГОСТ Р 34.13-2015. Введ. 01.01.2016. Москва: Стандартинформ, 2015. 38 с. (Национальный стандарт Российской Федерации). URL: http://protect.gost.ru/document.aspx?control=7&id=200971

5. Kaur G., Jagdev G. Implementation of DES and AES Cryptographic Algorithms in Accordance with Cloud Computing. *International Journal of Research Studies in Computer Science and Engineering* (IJRSCSE). 2017. Vol. 4. Issue 4. P. 1–14.

6. Информационная технология. Криптографическая защита информации. Блочные шифры [Текст]: ГОСТ Р 34.12-2015. Введ. 01.01.2016. Москва: Стандартинформ, 2015. 25 с. (Национальный стандарт Российской Федерации). URL: http://protect.gost.ru/document.aspx?control=7&id=200990

7. Georgoudis D., Leroux D., Chaves B. The FROG Encryption Algorithm. AES submission, 1998. URL: http://csrc.nist.gov/encryption/aes/round1/conf1/frog-slides.pdf

8. GRYPTRECproject//2000–2002. URL: http:www.ipa.go.jp/security/enc/CRYPTREC

9. Daemen J., Rijmen V. The Rijndael Block Cipher. AES submission. 1999. URL: http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf

10. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptossystems. *Communications of the ACM*. 1978. Vol. 21, No. 2. P. 120–126.

11. Riverst R.L. The RC5 Encryption Algorithm. Proc. Of the 2 Int. Workshop on FSE. 1994. P. 86–96.

12. Владимиров С.М., Габидулин Э.М., Колыбельников А.И., Квиевецкий А.С. Криптографические методы защиты информации: учеб. пособ. — Москва: МФТИ, 2016. 265 с.

13. Radziukevich M.L., Golikov V.F. Enhancing the secrecy of a cryptographic key generated using synchronized artificial neural networks1. *Informatics*. 2020. Vol. 17(1). P. 102–108.

14. Coifman R.R., Meyer Y., Wickerhauser M.V. Wavelet analysis and signal processing. Wavelet and their Application. Edited Jones and Darlett, B. Ruskaiand and other. 1992. P. 153–178.

15. Проценко М.М., Павлунько М.Я., Мороз Д.П. та ін. Методика фільтрації цифрових сигналів з використанням швидкого вейвлет-перетворення. *Сучасний захист інформації*. 2019. № 1(37). С. 64–69.

Надійшла до редакції 14.11.2020