УДК 681.3.067

Яремчук Ю.Є.

МЕТОД ГЕНЕРУВАННЯ ТА ПЕРЕВІРКИ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано метод та протокол генерування і перевірки цифрового підпису, що базуються на математичному апараті рекурентних V_k –послідовностей. Аналіз криптографічної стійкості представленого методу цифрового підписування показав, що він є більш стійким, ніж відомі аналоги. Також забезпечується можливість змінювати стійкість методу залежно від порядку послідовності, крім того, у порівнянні з відомими аналогами, метод має простішу процедуру завдання параметрів.

Ключові слова: захист інформації, криптографія, автентифікація, цифрове підписування, рекурентні послідовності.

Вступ

Розвиток комп'ютерних систем, мереж та засобів телекомунікацій значно розширив можливості застосування сучасних інформаційних технологій, систем електронного документообігу, що у свою чергу спричинило необхідність забезпечення захисту інформації не лише на рівні держави, але й у комерційній, фінансовій, банківській та інших сферах людської діяльності. При переході з паперового документообігу на електронний виникає проблема забезпечення цілісності та автентичності даних отриманих в електронному вигляді. На сьогодні задачі, пов'язані з автентифікацією даних та джерел повідомлень, найбільш ефективно та надійно вирішується за допомогою цифрового підписування [1–4].

Цифровий підпис у цифрових документах відіграє ту ж роль, що і підпис, поставлений від руки на паперових документах, тобто це дані, що приєднуються до повідомлення, яке передається, і підтверджують, що автор підпису (відправник-пидписант) склав та завірив дане повідомлення. Одержувач (перевіряльник) повідомлення або третя сторона за допомогою цифрового підпису може пересвідчитись, що автором повідомлення є саме власник підпису і що у процесі передавання не було порушено цілісність даних.

Цифрове підписування передбачає два етапи: генерування та перевірку цифрового підпису, що реалізується за певним протоколом [1]. Серед існуючих протоколів цифрового підписування найбільшого поширення отримали ті, що реалізують рандомізовані схеми з додаванням повідомлення, зокрема це методи Ель-Гамаля, Шнорра, DSA, ГОСТ 34.10 [1–3]. Ці методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Також недоліком цих методів цифрового підписування є те, що одна з частин підпису являє собою число (у більшості методів значення s), а не, скажімо, результат піднесення до степеня, що визначається цим числом (як, наприклад, інша частина підпису r у більшості методів), або результат інших обчислень над цими числами, які б значно ускладнювали зловмиснику його спроби щодо зламу і цим самим підвищували б стійкість цифрового підписування.

Враховуючи вищесказане, слід звернути увагу на математичний апарат рекурентних послідовностей [5, 6], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач та підвищувати стійкість на певних етапах криптографічних перетворень. Так в роботі [7] представлено метод автентифікації сторін взаємодії, який базується на рекурентних V_k –послідовностях і забезпечує підвищення стійкості у порівнянні з відомими аналогами.

Таким чином, актуальною є розробка методу генерування та перевірки цифрового підпису на основі рекурентних V_k –послідовностей, який би забезпечував підвищення рівня криптографічної стійкості.

Метод генерування та перевірки цифрового підпису на основі рекурентних V_k –послідовностей.

В [5] розглянуто V_k –послідовність, яка складається з V_k^+ –послідовності та V_k^- –послідовності.

V_k^+ –послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

V_k^- –послідовністю називається послідовність чисел, що обчислюються за формулою (2) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [5]

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (3)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [6]

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (4)$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють запропонувати такий метод генерування та перевірки цифрового підпису на їх основі.

Суть методу цифрового підписування, що пропонується (заявка на корисну модель № u 2013 06329 від 22.05.2013 р.), базується на використанні властивості (3) V_k –послідовності, яка дозволяє використовувати її для обчислення елементу $v_{n+m,k}$, а також для обчислення елементу $v_{-n+m,k}$. Крім того властивість (3) дозволяє реалізувати процедуру обчислення елементу $v_{n \cdot m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елементу $v_{-n \cdot m,k}$. Все це дає можливість створення такого методу цифрового підписування.

Спочатку відправник-підписант (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. При цьому він випадковим чином вибирає секретний ключ a, за допомогою якого обчислює, а потім передає одержувачу-перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

При генеруванні цифрового підпису для повідомлення M відправник-підписант вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення r як $r = v_{b,k}$. Далі він визначає значення s як $s = b \cdot h(M) + a \cdot r$ за допомогою обраної функції хешування h від повідомлення M, і обчислює для s елементи $v_{s+i,k}$, $i = \overline{-1,k-2}$. Після цього отриману множину цілих чисел $\{r; v_{s+i,k}, i = \overline{-1,k-2}\}$ він перетворює у цифровий підпис вигляду $DS = (0 \| r \| 0 \| v_{s-1,k} \| 0 \| v_{s,k} \| ... 0 \| v_{s+(k-2),k})$ і передає його разом з повідомленням M одержувачу.

При перевірці цифрового підпису одержувач спочатку обчислює $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, на основі відкритого ключа – елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, та отриманого від підписанта значення r. Потім він обчислює елемент $v_{b\cdot h(M),k}$ як $v_{b\cdot h(M),k}=v_{-a\cdot r+s,k}$, використовуючи залежність (3), і обчислює значення r' як $r'=v_{\left\lfloor\frac{b\cdot h(M)}{h(M)}\right\rfloor,k}$ та перевіряє, чи виконується $r\overset{?}{=}r'$. Якщо так, то підпис приймається, в іншому випадку – відкидається.

Не важко пересвідчитись, що для підпису, згенерованого згідно цього методу, перевірка $r\overset{?}{=}r'$ завжди буде виконуватись.

Виходячи з цього схема генерування та перевірки цифрового підпису за даним методом буде мати вигляд, представлений на рисунку 1.

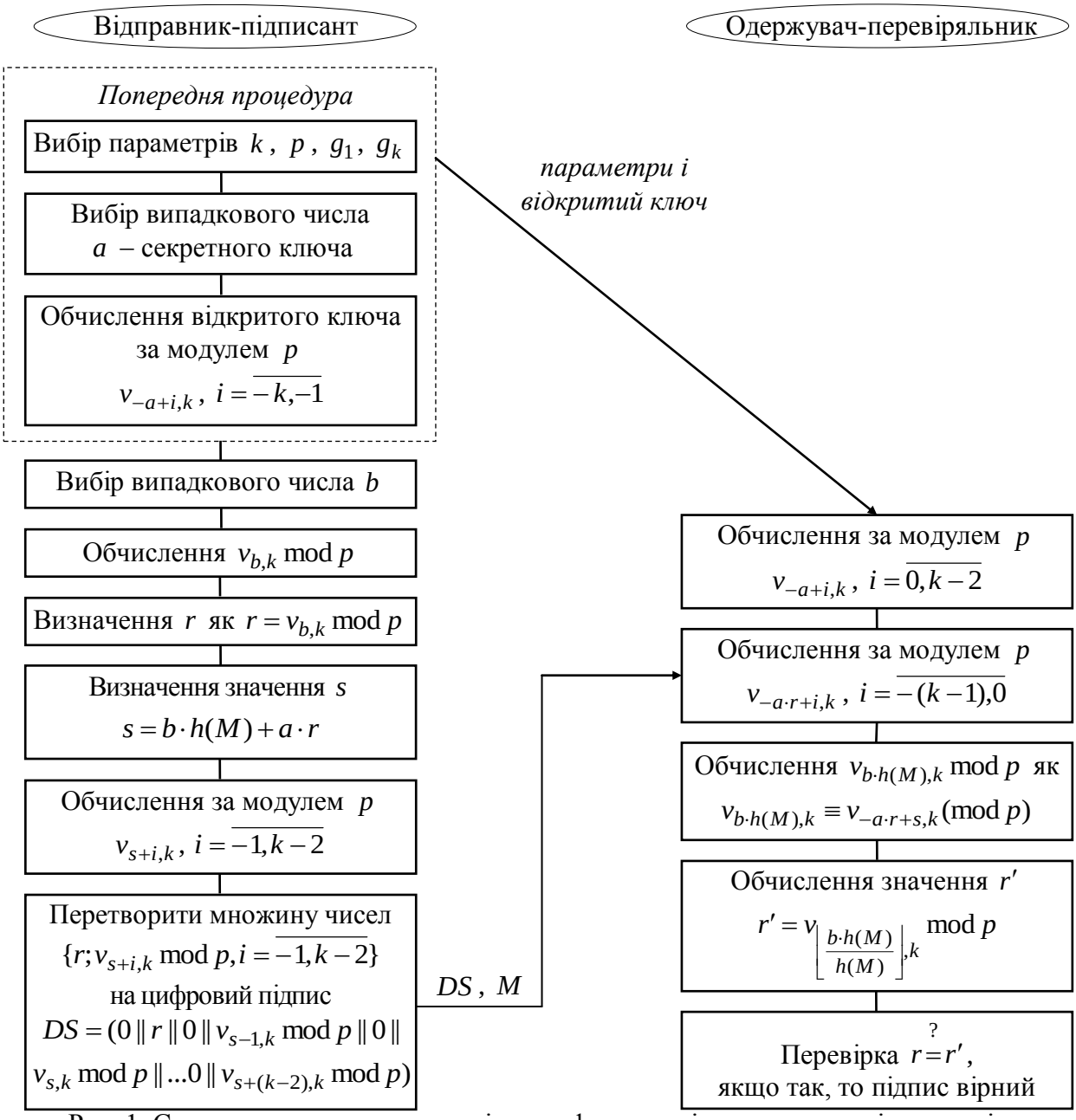

Рис. 1. Схема генерування та перевірки цифрового підпису на основі елементів V_k –послідовності.

Операція за модулем в схемі цифрового підписування використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Обчислення елементу $v_{b,k} \bmod p$ відправник може виконати попередньо, заздалегідь до безпосереднього формування цифрового підпису з повідомлення M.

В запропонованому методі генерування та перевірки цифрового підпису основні обчислення виконуються згідно залежності (3). Обчислення елементу $v_{n+m,k}$ згідно цієї залежності здійснюється на основі елементів $v_{n+i,k}$, $i = \overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i = \overline{-1,k-2}$.

В разі необхідності отримання певного послідовного набору елементів V_k–послідовності у кількості більшої ніж k, достатньо отримати будь-які послідовні k з них, оскільки інші можуть бути обчислені згідно формул (1) або (2) на основі вже отриманих.

Визначивши як можуть отримуватись елементи V_k–послідовності, що використовуються в методі цифрового підписування, отримаємо такий протокол генерування та перевірки цифрового підпису.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати g_1, g_k.

П.4. Відправнику передати параметри Одержувачу.

П.5. Відправнику вибрати випадкове число a – секретний ключ.

П.6. Відправнику обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i = \overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П.7. Відправнику передати відкритий ключ $v_{-a+i,k} \bmod p$, $i = \overline{-k,-1}$, Одержувачу.

П.8. Одержувачу обчислити за модулем p $v_{-a+i,k}$, $i = \overline{0,k-2}$, за формулою (1).

П.9. Відправнику вибрати випадкове число b.

П.10. Відправнику обчислити $v_{b,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.11. Відправнику визначити значення r як $r = v_{b,k} \bmod p$.

П.12. Відправнику визначити значення s як $s = b \cdot h(M) + a \cdot r$ за допомогою обраної функції хешування h від повідомлення M.

П.13. Відправнику обчислити за модулем p елементи $v_{s+i,k}$, $i = \overline{-1,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.14. Відправнику перетворити множину цілих чисел $\{r; v_{s+i,k} \bmod p, i = \overline{-1,k-2}\}$ у цифровий підпис вигляду $DS = (0 \| r \| 0 \| v_{s-1,k} \bmod p \| 0 \| v_{s,k} \bmod p \| ... 0 \| v_{s+(k-2),k} \bmod p)$ і передати його разом з повідомленням M Одержувачу.

П.15. Одержувачу обчислити за модулем p $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1),0}$, використовуючи алгоритм прискореного обчислення елементів $v_{-m \cdot n,k}$.

П.16. Одержувачу обчислити $v_{b \cdot h(M),k} \bmod p$ як $v_{b \cdot h(M),k} \equiv v_{-a \cdot r+s,k} (\bmod p)$ згідно залежності (3).

П.17. Одержувачу обчислити значення r' як $r' = v_{\left\lfloor \frac{b \cdot h(M)}{h(M)} \right\rfloor, k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{-m \cdot n, k}$.

П.18. Одержувачу перевірити, чи виконується $r \overset{?}{=} r'$, якщо так, то підпис вважати вірним.

У п.2 проводиться вибір параметру p, який є модулем при обчисленнях в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п.3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

У п.10 протоколу генерування та перевірки цифрового підпису відправнику необхідно здійснювати обчислення $v_{b,k} \bmod p$, а у п.13 – обчислення за модулем p елементів $v_{s+i,k}$, $i = \overline{-1, k-2}$. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які представлено в роботі [6].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i = \overline{-k, k-2}$, що виконуються відправником у п.6 протоколу цифрового підписування, на основі одного з запропонованих у тій же роботі [6] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п.15 одержувачу необхідно обчислювати за модулем p елементи $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1), 0}$. Для цього можна використати алгоритм прискореного обчислення елементів $v_{-m \cdot n,k}$, який представлено в роботі [7].

У п.17 одержувачу необхідно обчислювати за модулем p елемент $v_{\left\lfloor \frac{b \cdot h(M)}{h(M)} \right\rfloor, k}$. Це можна здійснювати як обчислення елементу $v_{\left\lfloor \frac{m \cdot n}{n} \right\rfloor, k}$ по аналогії з обчисленням елементу $v_{-m \cdot n,k}$ згідно алгоритму прискореного обчислення цих елементів представленого у роботі [7], але починати обчислення не з елементів $v_{-m+i,k}$, $i = \overline{-k, k-2}$, а з елементів $v_{m \cdot n+i,k}$ для тих же значень i.

Не важко помітити, що у випадку, якби $k = 1$, запропонований метод генерування та перевірки цифрового підпису став би дуже подібним на метод Ель-Гамаля.

Згідно відомого протоколу цифрового підписування Ель-Гамаля [8] центр довіри або відправник (підписант) вибирає і відкрито публікує просте число p та ціле число g, $1 < g < p$. Потім він вибирає випадкове число a, $1 \le a \le p-2$, як секретний ключ та обчислює $y = g^a \bmod p$ – відкритий ключ, який передається одержувачу (перевіряльнику). Після цього протокол цифрового підписування реалізується таким чином.

На етапі генерування підпису підписант вибирає випадкове число k, $1 \le k \le p-2$ і $НОД(k, p-1) = 1$, та обчислює $r = g^k \bmod p$ (ці обчислення можуть бути виконані і попередньо). Потім він обчислює $s = k^{-1}\left(h(M) - a \cdot r\right) \bmod (p-1)$, де h – функція хешування, і надсилає повідомлення M з підписом (r, s) одержувачу.

На етапі перевірки підпису перевіряльник спочатку перевіряє чи $0 < r < p$ та $0 < s < p-1$ і, якщо хоча б одна умова не виконується, то підпис відкидається. А потім, якщо обидві ці умови виконуються, підпис приймається тоді і лише тоді коли виконується рівняння $g^{h(M)} \bmod p \stackrel{?}{=} y^r r^s \bmod p$.

Проведемо аналіз запропонованого методу генерування та перевірки цифрового підпису на основі елементів V_k–послідовності та порівняємо його з відомим методом цифрового підписування Ель-Гамаля щодо криптографічної стійкості.

Здійснювати криптоаналіз запропонованого методу цифрового підписування на основі V_k–послідовності зловмисник може на основі відомих параметрів k, p, g_1, g_k, відкритого ключа $v_{-a+i,k} \bmod p$, $i = \overline{-k,-1}$, набору чисел $\{r; v_{s+i,k} \bmod p, i = \overline{-1,k-2}\}$ цифрового підпису та повідомлення M, які передаються від відправника до одержувача. Відповідно згідно методу Ель-Гамаля зловмиснику відомі параметри p, g, відкритий ключ $g^a \bmod p$, а також повідомлення M з підписом (r,s), які передаються одержувачу відправником.

В роботі [5] досліджувалась стійкість криптографічних перетворень, що базуються на використанні елементів V_k^+ та U_k – послідовностей, з яких видно, що складність отримання зловмисником індексу елемента рекурентної послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня. Тобто можна вважати, що ці обчислення знаходяться приблизно на одному ж рівні.

Виходячи з цього можна стверджувати, що метод генерування та перевірки цифрового підпису на основі V_k–послідовності криптографічно є більш стійким, ніж відомий метод Ель-Гамаля, оскільки в ньому замість передавання від відправника до одержувача числа s як частини підпису відповідно передаються елементи $v_{s+i,k} \bmod p$, $i = \overline{-1,k-2}$, тобто не саме число-індекс, а елементи рекурентної послідовності, обчислені для заданого індексу.

Перевагою запропонованого методу цифрового підписування на основі рекурентних послідовностей перед відомими методами щодо стійкості є також можливість змінювати параметр k, що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу цифрового підписування.

Також перевагою запропонованого методу генерування та перевірки цифрового підпису є те, що він має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Проведемо тепер порівняльний аналіз запропонованого методу генерування та перевірки цифрового підпису з відомим аналогом щодо обчислювальної складності.

З результатів дослідження складності обчислення елементів V_k–послідовності, які наведено в роботі [6], видно, що складність обчислення елементу V_k–послідовності за алгоритмом його прискореного обчислення є значно більшою, ніж за будь-якою аналітичною залежністю обчислення елементів цієї послідовності. Так само у відомому методі цифрового підписування Ель-Гамаля обчислювальна складність операції піднесення до степеня є значно більшою, ніж будь-якої іншої операції, що використовується в даному методі.

Аналіз запропонованого та відомого методів цифрового підписування показує, що згідно запропонованого методу необхідно п’ять разів проводити обчислення елементів V_k–послідовності за прискореним алгоритмом, а саме обчислення за модулем p різних наборів елементів з $v_{-a,k}$, $v_{b,k}$, $v_{s,k}$, $v_{-a\cdot r,k}$ та $v_{\left\lfloor \frac{b\cdot h(M)}{h(M)} \right\rfloor,k}$. Стільки ж, п’ять, необхідно

виконувати піднесень до степеня за модулем p згідно відомого методу Ель-гамаля: g^a, g^k, $g^{h(M)}$, y^r та r^s.

В роботі [6] проведено дослідження складності виконання алгоритмів прискореного обчислення елементів V_k –послідовності, з якого видно, що складність обчислення елементу цієї послідовності із заданим індексом має приблизно такий же рівень як і піднесення до заданого степеня того ж порядку, що й індекс.

Виходячи з цього, запропонований метод цифрового підписування на основі V_k –послідовності в цілому має приблизно такий же рівень обчислювальної складності, що і відомий метод Ель-Гамаля. При цьому слід відзначити, що розмір цифрового підпису згідно відомого методу є меншим, оскільки відправник передає лише саме число s, а не набір з k елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, як у запропонованому методі. Правда, цей недолік, може бути усунутий за рахунок зменшення криптографічної стійкості запропонованого методу до рівня відомого методу шляхом зменшення розміру чисел та елементів послідовності, який в основному визначається параметром p методу. Тоді зменшиться і розмір цифрового підпису і, як наслідок, зменшиться і обчислювальна складність запропонованого методу.

Слід також відзначити, що у запропонованому методі обчислення елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, можна здійснювати і на стороні одержувача, при цьому, як і у відомих аналогах, відправник буде передавати лише саме число-індекс s (заявка на корисну модель № u 2013 06332 від 22.05.2013 р.). Тоді рівень криптографічної стійкості запропонованого методу знизиться приблизно до рівня відомих аналогів, при цьому зменшиться обчислювальна складність методу.

Висновки. Представлено метод генерування та перевірки цифрового підпису на основі математичного апарату рекурентних V_k –послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елементу цієї послідовності з певним індексом. Також представлено протокол цифрового підписування для запропонованого методу, а також розглянуто можливість його реалізації.

Проведено порівняльний аналіз запропонованого методу генерування та перевірки підпису з відомим методом Ель-Гамаля щодо криптографічної стійкості, яке показало, що запропонований метод є більш стійким, ніж відомий аналог. При цьому порівняльний аналіз обчислювальної складності запропонованого методу показав, що він знаходиться приблизно на одному ж рівні з відомим аналогом.

Крім того запропонований метод дозволяє змінювати стійкість методу залежно від порядку послідовності k, а також має простішу процедуру завдання параметрів у порівнянні з відомими аналогами.

ЛІТЕРАТУРА

1. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

3. Молдавян, Н. А. Теоретический минимум и алгоритмы цифровой подписи / Н. А. Молдавян. – СПб.: БХВ-Петербург, 2010. – 304 с.

4. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеева, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

5. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю.Є. Яремчук // Захист інформації. – 2012. – № 4. – С. 120 – 127.

6. Яремчук Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань / Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 15, №1, 2013. – С. 14–22.

7. Яремчук Ю.Є. Методи автентифікації на основі рекурентних послідовностей / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.

8. El Gamal, T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms / T. ElGamal // Advances in Cryptology: Proceedings of CRYPTO 84. – Springer Verlag, 1985. – P. 1–18.

Надійшла: 22.08.2013р Рецензент: д.т.н., проф. Ленков С.В

УДК 621.391

Корчинский В.В., Казакова Н.Ф.

УСЛОВИЕ ОБЕСПЕЧЕНИЯ ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ ХАОТИЧЕСКИХ СИГНАЛОВ ПРИ ПЕРЕДАЧЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Рассмотрено условие обеспечения энергетической скрытности передачи конфиденциальной системы связи на основе сигнальных конструкций реализаций динамического хаоса. Показана возможность использования многоуровневых последовательностей в качестве расширяющих последовательностей информационного сигнала для повышения скрытности передачи. Проведено имитационное моделирование системы связи с хаотическими сигналами.

Ключевые слова: *с*крытность, база, канал, хаос, сигнал, сигнатура.

Обзор проблемы и постановка задачи. Одним из наиболее важных требований, предъявляемых к конфиденциальной системе связи (КСС) является обеспечение заданной помехозащищенности, которая характеризует способность системы выполнять свои задачи с заданным качеством в условиях радиоэлектронного подавления (РЭП) и несанкционированного доступа (НСД) [1]. РЭП и НСД организуется радиотехнической разведкой (РР) противоборствующей стороны, которая включает три основные задачи: обнаружения факта работы КСС; идентификация структуры и параметров сигналов-переносчиков; раскрытие смыслового содержания перехваченного сообщения.

Способность КСС противостоять мерам радиотехнической разведки (РР) называется скрытностью, которая является одним из главных показателей помехозащищенности. В соответствии с задачами радиоразведки выделяют следующие основные виды скрытности: энергетическая, структурная и информационная [1]. Другим важным показателем помехозащищенности является помехоустойчивость, которая характеризуется способностью системы связи нормально функционировать, выполняя задачи по приему информации в условиях действиях радиопомех, в том числе, преднамеренных.

Энергетическая скрытность направлена на существенное затруднение обнаружения сигнала работающей КСС средствами РЭП (разведывательным приемным устройством). Данный вид скрытности в основном обеспечивается за счет энергетической скрытности сигналов-переносчиков с базой $B >> 1$. Так в технологии многостанционного доступа с кодовым разделением каналов (Code Division Multiple Access – CDMA) для этой цели применяются шумоподобные сигналы (ШПС), формируемые на основе двоичных расширяющих последовательностей Уолша – метод DSSS (Direct Sequence Spread Spectrum). При этом закономерно, что увеличение энергетической скрытности передачи достигается за счет большей базы сигнала-переносчика, т.е. чем больше распределение энергии сигнала в большей полосе частот, тем меньше вероятность её обнаружения разведывательным приемным устройством РЭП на фоне помех.

В случае перехвата сообщения структурная скрытность направлена на затруднение измерения параметров сигнала-переносчика и идентификации структуры сигнала. Для повышения структурной скрытности целесообразно применение сигналов со сложной и изменяемой структурой, что даёт возможность, в перспективе, создавать сигналы-