УДК 621.391.7 **Яремчук Ю.Є.**

МЕТОД АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

У роботі розглянуто метод автентифікації сторін взаємодії на основі рекурентних V_k^+ та U_k-послідовностей та їх залежностей. Проведено дослідження представленого методу щодо обчислювальної складності та криптостійкості.

Ключові слова: захист інформації, криптографія, автентифікація, автентифікація сторін взаємодії, рекурентні послідовності.

Вступ. Для вирішення проблеми захисту інформації в інформаційно-комунікаційних системах від небажаного втручання з боку зловмисника застосовують криптографічні методи захисту [1, 2]. Історично криптографія виникла як наука про шифрування інформації [2, 3]. В класичній шенонівській моделі [4] системи секретного зв'язку мають двох учасників, які повністю довіряють один одному і передають між собою інформацію, що не призначена для сторонніх осіб. Таку інформацію називають секретною або конфіденційною, а задачу, яка тут виникає, називають задачею забезпечення конфіденційності або секретності від зовнішнього противника [3, 5]. Традиційно ця задача розв'язується за допомогою криптосистем.

Швидкі темпи розвитку засобів зв'язку та комп'ютерних мереж привели до широкого впровадження електронних банківських платежів та можливості обміну різного роду електронними документами. В зв'язку з цим у споживача можуть виникнути обґрунтовані сумніви відносно того, що отримана ним інформація створена потрібним джерелом, причому в такому вигляді, в якому вона дійшла до нього. Тобто необхідна гарантія того, що повідомлення надійшло з достовірного джерела та в неперекрученому вигляді. Така гарантія отримала назву забезпечення цілісності інформації [3, 5] і складає другу задачу криптографії.

Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації розробляються криптографічні протоколи . Найбільш розповсюдженими є два типи криптографічних протоколів автентифікації та цифрового підписування . На сьогодні задача забезпечення цілісності є не менш, а в деяких випадках і більш актуальною, ніж задача конфіденційності інформації.

Стосовно автентифікації, то в основному розрізняють [3] автентифікацію сторін або учасників взаємодії, яку ще іноді називають ідентифікацією, а також автентифікацію джерел інформації. В першому випадку автентифікація означає перевірку однією з сторін того, що взаємодіюча з нею сторона саме та, за яку вона себе видає. В другому випадку автентифікація означає підтвердження того, що вихідний документ був створений саме заявленим джерелом.

В загальному вигляді в схемі автентифікації сторін взаємодії [5] існує два учасника одна сторона, яка повинна довести свою автентичність та друга сторона, яка цю автентичність повинна перевірити. Перша сторона має два ключа загальнодоступний K_1 та секретний K_2. Другій стороні необхідно довести, що вона знає K_2, причому зробити це таким чином, щоб це доведення можна було б перевірити знаючи лише K_1. При такій схемі забезпечується доведення автентичності з нульовим розголошенням.

Теоретичні основи схем автентифікації були закладені в роботі Сіммонса [8]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1, 2, 5, 6]. Ці методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Крім того, в цих методах, окрім передавання параметрів та відкритого ключа, необхідно виконувати триетапне передавання інформації, що також створює певні труднощі.

Далі пропонується метод автентифікації, який в певній мірі усуває вказані труднощі.

Математичний апарат на основі рекурентних послідовностей для розробки методу автентифікації. Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [9]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де $a_1, a_2, ..., a_k$ коефіцієнти, k порядок послідовності, виходячи з початкових елементів u_0, $u_1, ..., u_k$.

Назвемо послідовність чисел, що обчислюються за формулою

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

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 V_k^+ послідовністю.

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з $n = 0$. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n, починаючи з деякого значення $n = l$. Обчислення елементів такої послідовності буде здійснюватись таким чином

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

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

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

В окремому випадку, коли $m = n$ залежність (3) буде мати такий вигляд

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

З наведених аналітичних залежностей V_k^+ послідовності видно, що для довільного додатного номеру n обчислення елементу $v_{n,k}$ може здійснюватись за формулою (1). Однак, безпосереднє обчислення $v_{n,k}$ за цією формулою є повільним, а тому не може бути використано для великих значень n. Це створює проблему, оскільки при розробці методу шифрування доцільним є використання саме великих значень індексу елемента послідовності. Виникає необхідність у більш швидкому методі обчислення елементу $v_{n,k}$.

В зв'язку з цим пропонується спосіб обчислення $v_{n,k}$, який базується на тій же ідеї, що і бінарний метод [10] піднесення до степеня. Скористаємось даним методом для отримання адитивного ланцюжка

$$1 = c_0, c_1, c_2, ..., c_t = n.$$

Якщо записати n в двійковій системі числення як $n = \sum_{i=0}^{t} \alpha_{t-i} 2^{t-i}$, то для кожного $i = \overline{1,t}$ правило отримання адитивного ланцюжка, починаючи з c_1, буде таким

- якщо значення α_{t-i} дорівнює 0, то $c_i = 2c_{i-1}$;
- якщо значення розряду α_{t-i} дорівнює 1, то $c_i = 2c_{i-1} + 1$.

Як наслідок, дійшовши до крайнього правого розряду n отримаємо $c_t = n$.

Звідси, обчислення $v_{n,k}$ буде зводитись до послідовного обчислення $v_{c_i,k} = v_{2c_{i-1}+1,k}$ або $v_{c_i,k} = v_{2c_{i-1},k}$.

Обчислення $v_{c_i,k} = v_{2c_{i-1},k}$ будемо здійснювати згідно залежності (4), а $v_{c_i,k} = v_{2c_{i-1}+1,k}$ будемо отримувати, обчислюючи спочатку $v_{2c_{i-1},k}$, а потім $v_{2c_{i-1}+1,k}$ за формулою (1).

З (4) видно, що для отримання елементу $v_{2n,k}$ використовуються елементи $v_{n+k-2,k},...,v_{n-(k-2),k},v_{n-(k-1),k}$. Тобто на кожному кроці необхідно визначати та зберігати набір з $2k-2$ елементів. Розглянемо обчислення цих елементів.

Елементи $v_{2n,k},v_{2n-1,k},...,v_{2n-(k-3),k},v_{2n-(k-2),k}$ можуть бути обчислені згідно залежності (3) відповідно як $v_{n+n,k},v_{n+(n-1),k},...,v_{n+(n-(k-3)),k},v_{n+(n-(k-2)),k}$.

Елемент $v_{2n-(k-1),k}$ не може бути обчислений згідно залежності (3), оскільки для його обчислення, окрім елементів, які є в наведеному вище наборі, потрібен елемент $v_{n-k,k}$. Розширення цього набору елементів елементом $v_{n-k,k}$ не бажано, тому що для обчислення $v_{2n-k,k}$ буде потрібен елемент $v_{2n-(k+1),k}$. Щоб усунути цей недолік будемо обчислювати елемент $v_{2n-(k-1),k}$ за формулою (2).

В такому випадку необхідним є елемент $v_{2n+1,k}$. Цей елемент може бути обчислений згідно залежності (3). При цьому набір необхідних елементів буде розширений елементом $v_{n+k-1,k}$.

Елементи $v_{2n+k-1,k},...,v_{2n+3,k},v_{2n+2,k}$ можуть бути отримані на основі вже обчислених елементів $v_{2n+1,k},v_{2n,k},...,v_{2n-(k-3),k},v_{2n-(k-2),k}$, за формулою (1).

Таким чином, для обчислення елементу $v_{2n,k}$ на кожному кроці необхідно визначати та зберігати набір з $2k-1$ елементів.

Позначивши l як поточне значення індексу елементу V_k^+ послідовності, маємо такий алгоритм прискореного обчислення елементів цієї послідовності для додатних n.

П.1. Провести початкову ініціалізацію: $i \leftarrow t$; $l \leftarrow 1$; присвоїти елементам $v_{l+k-1,k},...,v_{l-(k-2),k},v_{l-(k-1),k}$ відповідні значення V_k^+ - послідовності.

П.2. $i \leftarrow i-1$.

П.3. $l \leftarrow 2l$.

П.4. Обчислити нові значення $v_{l+1,k},...,v_{l,k},...,v_{l-(k-3),k},v_{l-(k-2),k}$ за модулем p, використовуючи (3).

П.5. Обчислити елемент $v_{l-(k-1),k}$ за модулем p, використовуючи (2).

П.6. Якщо $k>2$, то обчислити елементи $v_{l+k-1,k},...,v_{l+k-2,k},...,v_{l+3,k},v_{l+2,k}$ за модулем p, використовуючи (1).

П.7. Якщо $\alpha_i = 0$, то перейти до п.10.

П.8. $l \leftarrow l+1$.

П.9. Обчислити нові значення $v_{l+k-1,k},...,v_{l-(k-2),k},v_{l-(k-1),k}$ шляхом присвоювання кожному попередньому елементу значення наступного за ним елементу та обчислення за модулем p останнього елементу $v_{l+k-1,k}$ за формулою (1), використовуючи тільки-но обчислені елементи.

П.10. Якщо $i-1 \neq 0$, то перейти до п.3, інакше завершити роботу алгоритму.

Таким чином представлено, а також отримано аналітичні залежності та алгоритми обчислення елементів V_k^+ послідовності. Ця послідовність є окремим випадком більш узагальненої послідовності, оскільки значення більшості початкових елементів нульові.

Якщо дозволити, щоб ці початкові елементи приймали будь-які значення, то отримаємо такий варіант узагальненої послідовності.

Назвемо послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \tag{5}$$

для початкових значень $u_{0,k} = g_1, u_{1,k} = g_2, u_{2,k} = g_3, ..., u_{k-1,k} = g_k$, де $g_1, g_2, g_3, ..., g_k$ - цілі числа; n і k цілі додатні числа U_k послідовністю.

Для будь-яких цілих додатних n, m та k отримано таку залежність

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k} . \tag{6}$$

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримано залежність, яка дозволяє обчислювати елементи U_k послідовності тільки на основі елементів V_k^+ послідовності

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} . \tag{7}$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити метод автентифікації сторін взаємодії на їх основі.

Метод автентифікації на основі рекурентних V_k^+ та U_k послідовностей.

Суть методу автентифікації, що пропонується, базується на аналітичній залежності (6), яка дозволяє обчислити елемент $u_{n+m,k}$ двома шляхами: або використовуючи елементи $v_{m+i,k}$, $i = \overline{-1, k-2}$, та $u_{n-i,k}$, $i = \overline{0, k-1}$, або використовуючи елементи $v_{n+i,k}$, $i = \overline{-1, k-2}$, та $u_{m-i,k}$, $i = \overline{0, k-1}$. Це дає можливість створення такого методу автентифікації сторін взаємодії.

Спочатку Перша сторона, що повинна довести свою автентичність, виконує попередню процедуру обчислення ключів. Для цього вона випадковим чином вибирає секретний ключ a, після чого обчислює і передає Другій стороні відкритий ключ $u_{a-i,k}$, $i = \overline{0, k-1}$.

Коли Друга сторона бажає перевірити автентичність Першої сторони, вона вибирає випадкове число b, обчислює $u_{b-i,k}$, $i = \overline{0, k-1}$, і передає отриманий набір елементів Першій стороні. Перша сторона, прийнявши цей набір елементів, здійснює на їх основі обчислення $u_{b+a,k}$. В цей же час Друга сторона обчислює $u_{a+b,k}$. Потім Перша сторона передає отримане значення $u_{b+a,k}$ Другій стороні, яка звіряє його зі значенням $u_{a+b,k}$, ідентифікуючи таким чином Першу сторону.

Виходячи з цього схема автентифікації сторін взаємодії за даним методом буде мати такий вигляд (рис.1).

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

Відповідно до запропонованого методу автентифікації основні обчислення виконуються згідно залежності (6). Для обчислення елементу $u_{n+m,k}$ згідно цієї залежності потрібні елементи $v_{m+i,k}$, $i = \overline{-1, k-2}$, та елементи $u_{n-i,k}$, $i = \overline{0, k-1}$. Обчислення останнього набору елементів здійснюється згідно залежності (7), для чого необхідно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1, -1}$. Звідси виходить, що всього для обчислення елементу $u_{n+m,k}$ згідно залежності (6) потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1, k-2}$. Задача знаходження цих елементів

зводиться до отримання будь-яких послідовних k з них, оскільки інші можуть бути обчислені за формулами (1) або (2) на основі вже отриманих.

Визначивши обчислення за усіма залежностями, що використовуються в методі автентифікації, отримаємо такий протокол автентифікації сторін взаємодії.

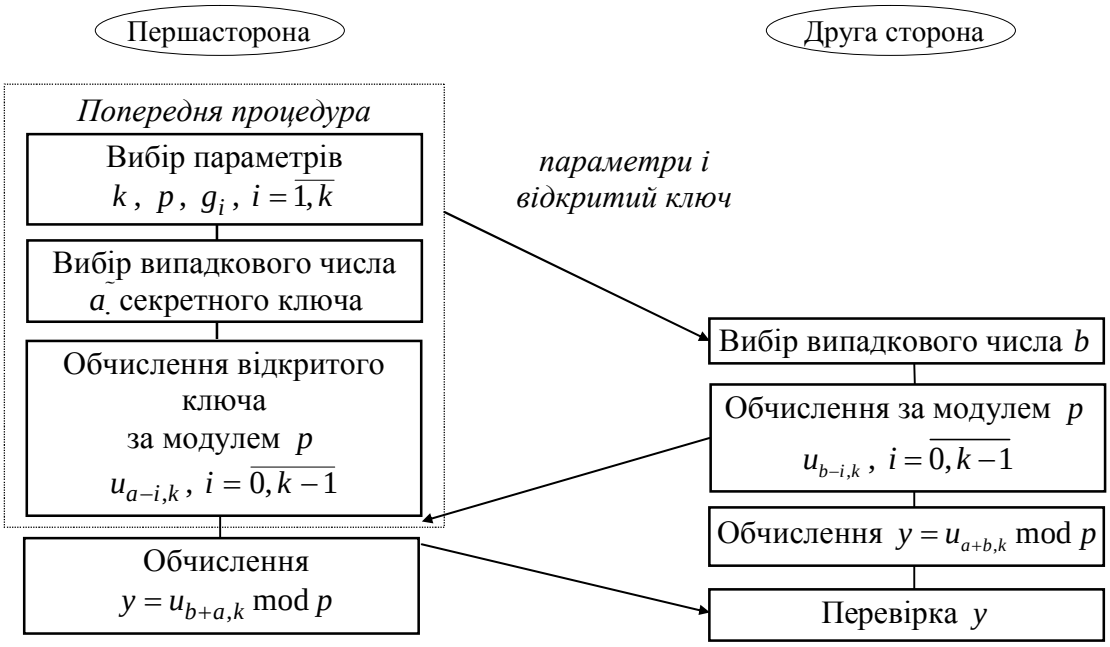

Рис. 1. Схема автентифікації сторін взаємодії на основі елементів U_k послідовності.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати $g_1, g_2, ..., g_k$.

П.4. Першій стороні передати параметри Другій стороні.

П.5. Першій стороні вибрати випадкове число a секретний ключ.

П.6. Першій стороні обчислити за модулем p $v_{a+i,k}$, $i=\overline{-(k-1),k-2}$.

П.7. Першій стороні обчислити за модулем p $v_{a+i,k}$, $i=\overline{-2k+1,-k}$, за формулою (2).

П.8. Першій стороні обчислити відкритий ключ за модулем p $u_{a-i,k}$, $i=\overline{0,k-1}$, згідно залежності (7).

П.9. Першій стороні передати відкритий ключ Другій стороні.

П.10. Другій стороні вибрати випадкове число b.

П.11 Другій стороні обчислити за модулем p $v_{b+i,k}$, $i=\overline{-(k-1),k-2}$.

П.12. Другій стороні обчислити за модулем p $v_{b+i,k}$, $i=\overline{-2k+1,-k}$, за формулою (2).

П.13. Другій стороні обчислити за модулем p $u_{b-i,k}$, $i=\overline{0,k-1}$, згідно залежності (7).

П.14. Другій стороні передати обчислені за модулем p $u_{b-i,k}$, $i=\overline{0,k-1}$, Першій стороні.

П.15. Першій стороні обчислити $y=u_{b+a,k} \bmod p$, а Другій стороні $y=u_{a+b,k} \bmod p$ згідно залежності (6).

П.16. Першій стороні передати значення y Другій стороні.

П.17. Другій стороні звірити отримане від Першої сторони значення y з тим значенням, що вона обчислила в п.15.

В 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.

В п.3 відбувається вибір параметрів g_i, $i=\overline{1,k}$. 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.

Визначимо тепер обчислювальну складність представленого протоколу автентифікації сторін взаємодії.

Слід зазначити, що в протоколі Перша сторона виконує попередню процедуру лише один раз перед безпосереднім використанням протоколу, обчислюючи за модулем p елементи $v_{a+i,k}$, $i=\overline{-2k+1,k-2}$, та на їх основі відкритий ключ - елементи $u_{a-i,k}$, $i=\overline{0,k-1}$, згідно залежності (7). Тобто при безпосередньому доведенні своєї автентичності Перша сторона обчислює лише $y=u_{b+a,k} \bmod p$ на основі отриманих раніше елементів в попередній процедурі та елементів $u_{b-i,k}$, $i=\overline{0,k-1}$, що кожного разу передаються від Другої сторони. Тому складність обчислень за протоколом буде визначатись в основному складністю обчислень з боку Другої сторони, яка перевіряє автентичність першої.

Складність обчислень за протоколом з боку Другої сторони визначається складністю обчислень за модулем p елементів $v_{b+i,k}$, $i=\overline{-(k-1),k-2}$, елементів $v_{b+i,k}$, $i=\overline{-2k+1,-k}$, за формулою (2), елементів $u_{b-i,k}$, $i=\overline{0,k-1}$ згідно залежності (7), та елементу $u_{a+b,k}$ згідно залежності (6). Обчислення першого набору елементів може бути здійснено за методом прискореного обчислення елементів V_k^+–послідовності, який було розглянуто вище. Встановлено, що складність обчислень даного набору елементів складає приблизно $H^2q\cdot[6H(k^2+k)+3(3k^2+k)]$ операцій над машинними одиницями інформації, де H кількість машинних одиниць інформації для зберігання великого числа, q кількість розрядів машинної одиниці інформації.

Обчислення інших елементів V_k^+ та U_k - послідовностей за модулем p згідно залежностей (2), (6) та (7) потребує виконання приблизно k^2+4k множень, k^2 додавань та k віднімань над машинними одиницями інформації. Враховуючи оцінки складності виконання арифметичних операцій за модулем над числами великої розрядності, складність обчислень згідно залежностей (2), (6) та (7) буде складати приблизно $6H(H+1)(k^2+4k)+2Hk^2(H+1)+3Hk(H+1)$ операцій над машинними одиницями інформації. Виходячи з того, що при реалізації криптографічних методів в сучасних комп'ютерних системах оперують ключами, що мають розмір 1024 і більше розрядів $(Hq\geq 1024)$, отримана оцінка буде значно меншою за оцінку складності обчислення набору елементів $v_{b+i,k}$, $i=\overline{-(k-1),k-2}$, а тому може не враховуватись в загальній оцінці складності всього протоколу автентифікації.

Таким чином складність виконання запропонованого протоколу автентифікації з боку Другої сторони буде складати приблизно $H^2q\cdot[6H(k^2+k)+3(3k^2+k)]$ операцій над машинними одиницями інформації.

Порівнюючи запропонований метод автентифікації з відомими методами Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра відносно складності виконання автентифікації слід відзначити таке. В запропонованому методі Першій стороні і Другій стороні необхідно виконувати обчислення певного елементу U_k послідовності по одному разу, в той час як за відомими методами їм необхідно виконувати піднесення до степеня по два рази. Враховуючи

результати аналізу, які показали, що складність обчислення певного елементу U_k послідовності має той же порядок, що і складність піднесення до заданого степеня, то можна стверджувати, що представлений метод має приблизно вдвічі меншу складність обчислень, ніж відомі методи автентифікації. Крім того запропонований метод має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Слід також відмітити те, що у відомих методах автентифікації, окрім передавання параметрів, необхідно виконувати три передавання інформації: два від першої сторони, яка доводить свою автентичність, до другої сторони, яка цю автентичність перевіряє, і одне передавання від другої сторони до першої, в той час як за представленим методом достатнім є лише два передавання: по одному з кожного боку.

Проведено дослідження криптостійкості представленого методу автентифікації сторін взаємодії, яке показало що запропонований метод автентифікації теоретично є криптостійким і має принаймні не менший рівень стійкості, ніж відомі методи.

Висновки. Запропоновано метод автентифікації сторін взаємодії, який базується на рекурентних V_k^+ та U_k послідовностях та отриманих для них залежностях. У порівнянні з відомими методами Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра цей метод має простішу процедуру завдання параметрів та приблизно вдвічі меншу складність обчислень. Крім того, у відомих методах, окрім передавання параметрів, безпосередньо під час автентифікації необхідно виконувати три етапи передавання інформації, в той час як у представленому методі лише два. Результати дослідження запропонованого методу з точки зору теоретичної криптостійкості показали, що метод є стійким і має не менший рівень стійкості, ніж відомі методи.

ЛІТЕРАТУРА

1. 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.

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

3. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, Черемушкин А.В. – М: Гелиос АРВ, 2001. – 480 с.

4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Tech. Jour. - 1949. - V.28, №11.

5. Ященко В.Б. Введение в криптографию / Под общ. ред. В.Б. Ященко. - М.: МЦНМО: «ЧеРо», 2000. – 236 с.

6. Петров А.А. Компьютерная безопасность. Криптографические методы защиты / Петров А.А. – М.: ДМК, 2000. – 448 с.

7. Брассар Ж. Современная криптология / Брассар Ж. - М.: ПОЛИМЕД, 1999. – 176 с.

8. Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411-431.

9. Маркушевич А.И. Возвратные последовательности / А.И. Маркушевич. - М.: Наука, 1975. - 48 с.

10. Кнут Д. Искусство программирования для ЭВМ. Т2. Получисленные алгоритмы / Кнут Д. - М.: Вильямс, 2004. - 832 с.

Надійшла: 27.12.2012

Рецензент: д.т.н., проф. Хорошко В.О.