УДК 004.052.42

[1]Мухін В. Є., [1]Лефтеріос Захаріудакіс, [2]Герасименко О. Ю., [1]Козерацький М. С.
[1]Національний технічний університет України «Київський політехнічний інститут» ім. Ігора Сікорського
[2]Київський національний університет імені Тараса Шевченка

МЕТОД ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА ОСНОВІ КОНЦЕПЦІЇ "НУЛЬОВИХ ЗНАНЬ"

В статті представлено метод реалізації теоретично строгої ідентифікації віддалених користувачів або термінальних пристроїв багатокористувацьких систем, що реалізує концепцію "нульових знань". Метод має за основу використання математичних незворотних перетворень теорії чисел. Передбачені методом процедури реєстрації користувача та його ідентифікації ілюстровані числовим прикладом. За результатами експериментальних досліджень проведене порівняння запропонованого методу та відомих.

***Ключові слова*:** багатокористувацькі системи, ідентифікація віддалених користувачів, концепція ідентифікації "нульових знань", модулярне експоненціювання

Mukhin V. Ye., Zacharioudakis Eleftherios, Herasymenko O. Yu., Kozeratskiy M. S. Method zero-knowledge identification of remote users. In article the new method for implementation of theoretical strong identification of remote abonents or tample-resistant devices of multiuser systems, based on zero-knowledge conception is presented. The need for efficient remote users identification procedure is hence explained. The mathematic background of proposed method consist of using the number theory irreversible transformation. The main peculiarities of proposed method consist of that identification process only takes a single cycle of information exchanges between the user and the system and hence reduces the overhead of the authentication process while minimizing the danger of malicious third parties intervening during this process. Apart from it allows to speed up of identification process for software and hardware implementation. The technology of mathematical transformations whose are provided by proposed method are set forth clearly. A numerical example for designed procedures of user registration and user is given. It has been shown that

An experimental comparison of the identification processing time of both the proposed and known methods is presented, that demonstrates the improvements attained.

Keywords: multi user systems, remote users identification, methods of strong identification, zero-knowledge identification conception, modular exponentiation

1. Вступна частина. ***Постановка задачі.*** Інтегровані системи зберігання та обробки даних з колективним доступом відіграють зростаючу роль в глобальних процесах інформаційної інтеграції. Розвиток таких систем значною мірою залежить від ефективності реалізації в них функцій захисту інформації та розподілення прав доступу. Ключова роль в вирішенні цієї проблеми належить засобам ідентифікації абонентів. Виходячи з цього, вдосконалення таких засобів являє собою важливим та актуальним для розвитку сучасних інформаційних та мережевих технологій.

Високий рівень ефективності ідентифікації віддалених абонентів досягається як результат певного компромісу між рівнем захищеності від несанкціонованого доступу та швидкістю ідентифікації. Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, що намагається реалізувати незаконний доступ до ресурсів системи. В першому наближенні процедура ідентифікації має задовольняти таким вимогам:

1) Організація зберігання ідентифікуючої інформації має бути такою, щоб одна її частина зберігалася у абонента, а друга – в системі і кожна з цих частин не була б самодостатньою для доступу до ресурсів системи.

2) Пароль має вибиратися абонентом, не зберігатися в пам'яті, а вводитися при кожному сеансі та не бути достатнім для реалізації доступу до ресурсів.

3) Мінімальне використання відкритих ліній передачі даних – найбільш вразливого місця з точки зору незаконного проникнення до ресурсів системи.

4) Ідентифікаційна посилка абонента при кожному сеансі підключення до системи має змінюватися.

5) Об'єм секретної інформації, що зберігається в системі і використовується для ідентифікації, має бути якомога меншим з тим, щоб надати можливість збереження такої інформації в спеціальній захищеній на апаратному рівні пам'яті.

6) Ідентифікаційна інформація при передачі по відкритій лінії має шифруватися.

7) Розпізнавання легальних абонентів та контроль прав доступу до ресурсів для них має виконуватися різними механізмами захисту.

В основі більшості протоколів ідентифікації віддалених абонентів лежить теоретична концепція ”нульових знань”. Сутність цієї концепції полягає в тому, що для доведення своєї автентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента.

При цьому в системі не зберігається ніякої секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань”. Важливим є те, що при кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

Таким чином, концепція нульових знань в теоретичному плані найбільш повною мірою відповідає сформульованим вище вимогам щодо системи ідентифікації абонентів. Концепція нульових знань передбачає використання теоретично незворотних криптографічних перетворень. Це означає, що існує алгоритм перетворення в прямому напрямку, але принципово неможливим є аналітичне віднаходження алгоритму зворотного перетворення. В існуючих схемах ідентифікації на основі концепції нульових знань для реалізації такого перетворення використовуються аналітично нерозв’язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування.

Аналіз літературних джерел. На практиці найбільшого поширення набули методи FESIS [1], Guillou-Quisquater [2] та Schnorr [3].

Суть методу FESIS полягає в наступному. Користувач вибирає два простих числа p і q, та обчислює модуль $m=p\cdot q$. Для генерації відкритого та закритого ключів користувач вибирає число v, що є квадратичним лишком по модулю m. Іншими словами, користувач вибирає таке v, для якого існує таке x що $x^2 \bmod m = v$ і існує v^{-1} таке, що $v\cdot v^{-1} \bmod m = 1$. Віднаходиться найменше s для якого має місце $s^2 \bmod m = v^{-1}$. Число v разом з модулем m утворюють відкритий ключ, а число s – закрий ключ.

При реєстрації користувач посилає системі свій відкритий ключ: число v та модуль m.

В циклі ідентифікації користувач вибирає випадкове число r та обчислює значення $x = r^2 \bmod m$, після чого обчислене значення x відсилає в систему. Система ініціює виконання t циклів акредитації, в кожному з яких виконуються такі дії:

1) Система посилає користувачу випадковий біт b.

2) Якщо b=0, то користувач посилає в систему число r, в протилежному випадку, тобто якщо b=1, користувач обчислює з використанням закритого ключа s значення $y = r\cdot s \bmod m$ і відсилає його системі.

3) Якщо b=0, то система перевіряє $x = r^2 \bmod m$, а якщо b=1, то система виконує перевірку $x = y^2\cdot v \bmod m$, переконуючись, що абонент знає $s = \sqrt{v^{-1}}$.

Для сторони, що здійснює спробу незаконного отримання доступу до ресурсів системи під виглядом користувача не відомі компоненти закритого ключа: число v та модуль m користувача. Відповідно сторонній зловмисник, перехоплюючи h циклів ідентифікації отримає дані з h_1 циклів при b=0 та h_2 циклів при b=1, $h=h_1+h_2$. Таким чином, зловмисник має в своєму розпорядженні сукупність пар чисел $\langle r_i, x_i\rangle$, $\forall i\in\{1,2,\ldots,h_1\}$: $x_i = r_i^2 \bmod m$ $\langle r_j, y_j\rangle$, та $\forall j\in\{1,2,\ldots,h_2\}$: $y_j = r_j\cdot s \bmod m$. Сукупність пар $\langle r_i, x_i\rangle$ потенційно може бути використана для підбору модуля m. Сукупність пар $\langle r_j, y_j\rangle$ може бути використана для підбору закритого ключа s. Обидві вказані задачі в математичному сенсі еквівалентні розкладанню числа на два співмножника і при розрядностях більших за 1024 потребують ресурсів. що виходять за рамки практичної доцільності.

Якщо зловмисник знаходиться в самій системі, тобто знає відкритий ключ, тобто число v та модуль m користувача, то зловмисник може вибрати будь-яке g та обчислити $\xi= g^2 \bmod m$; послати системі ξ в якості x. Якщо зловмисник отримає від системи біт запиту b=1, то він відсилає системі згенероване ним число g. Система перевіряє той факт, що $\xi= g^2 \bmod m$.

Проте, якщо зловмисник отримає від системи біт запиту b=1, то він має послати у відповідь системі обчислене з використанням закритого ключа s значення $y = g \cdot s \bmod m$. Очевидно, що не знаючи закритого ключа s, зловмисник не зможе обчислити коректне значення s. Підбор зловмисником закритого ключа s в математичному сенсі еквівалентно задачі віднаходження значення v^{-1} по відомому v. В свою чергу, ця задача може бути розв'язана лише за умови, що зловмисник знає складові співмножники p і q, такі, що $m=p\cdot q$. Проте, система не знає цих співмножників і, відповідно, задача підбору сеансового паролю зловмисником, що знаходиться в системі, практично не може бути реалізована.

Найбільш значимими для практики недоліками схеми ідентифікації FFSIS є необхідність в декількох циклах акредитації, що, в свою чергу, потребує відповідності кількості сеансів передачі даних. Час, потрібний для здійснення сеансу передачі даних між користувачем та системою суттєвим чином залежить від поточного трафіку в комп'ютерній мережі і на порядки перевищує час виконання системою обчислень, пов'язаних з ідентифікацією користувача. Проведення декількох коротких сеансів передачі даних при ідентифікації кожного користувача значно впливає на пропускну здатність мережевого інтерфейсу систем колективного доступу. Крім того, наявність прогнозованих декількох сеансів передачі даних з конкретним користувачем відкриває потенціальні можливості для зловмисників ефективно завадити успішному проведенню циклу ідентифікації. Таким чином, необхідність в декількох сеансах передачі даних суттєвим чином сповільнює процес ідентифікації користувача.

Крім методу FFSIS та його модифікацій [3], широкого розповсюдження в системах колективного доступу набув метод Guillou-Quisquater [2], який також реалізує теоретичну концепцію строгої ідентифікації "нульових знань". Згідно з ним користувач вибирає відкритий пароль ϑ. До складу відкритого ключа системи входить також модуль m, що формується користувачем як добуток $m = p\cdot q$ двох простих чисел p і q, що тримаються в секреті. Користувачем підбираються такі числа v і B, що $(\vartheta\cdot B^v) \bmod m = 1$. При реєстрації користувач пересилає системі відкритий пароль ϑ та модуль m.

Цикл ідентифікації складається з наступної послідовності дій:

1) Користувач формує випадкове число r.

2) Користувач обчислює сеансовий пароль у вигляді: $P = r^v \bmod m$ і пересилає обчислений код P до системи.

3) Система, отримавши код P випадковим чином генерує число d, для якого виконується умова $0<d<m$-1; число d система пересилає користувачу.

4) Користувач обчислює $G = r\cdot B^d \bmod m$ і відсилає обчислений код G системі.

5) Система обчислює $Q=G^v\cdot\vartheta^d \bmod m$. Користувач вважається легальним, якщо виконується умова $Q=P$.

Метод має в якості математичної основи еквівалентність перетворень:

$Q= G^v\cdot\vartheta^d \bmod m=(r\cdot B^d)^v\cdot \vartheta^d \bmod m=r^v\cdot B^{d\cdot v}\cdot\vartheta^d \bmod m = r^v\cdot(\vartheta\cdot B^v)^d \bmod m = r^v \bmod m = P.$

Основним недоліком розглянутого методу в сучасних умовах є використання декількох сеансів обміну даними між користувачем та системою, а також необхідність виконання операції модулярного експоненціювання користувачем безпосередньо в процесі ідентифікації. Це суттєвим чином збільшує час ідентифікації користувача.

Метод Schnorr [3] також передбачає вибір користувачем двох простих чисел p та q причому, q має бути подільником p-1. Вибирається число a таке, що $a^q \bmod p$ =1. Вибирається випадкове число s менше за q : $s<q$, яке являє собою секретний ключ користувача. Далі користувачем обчислюється відкритий ключ у вигляді: $v=a^{-s} \bmod p$, який передається системі під час реєстрації.

Цикл ідентифікації користувача складається з наступної послідовності дій:

1) Користувач генерує випадкове число r : $r<q$, після чого обчислює число $x=a^r \bmod p$.

2) Код x відсилається користувачем в систему.

3) Система генерує випадкове h-розрядне число e і відправляє його користувачеві.

4) Користувач обчислює $y=(r+s\cdot e) \bmod q$ та відправляє отримане значення в систему.

5) Система обчислює $\Theta = a^{y} \cdot v^{e} \bmod p$ і порівнює обчислене значення з одержаним кодом x: якщо $\Theta = x$, то права доступу користувача вважаються легітимними.

Особливістю розглянутого методу ідентифікації, що реалізує концепцію "нульових знань" є використання групи чисел менших за q відносно невеликої розрядності, що дозволяє суттєво зменшити обчислювальну складність операцій, пов'язаних з процесом ідентифікації. З іншого боку відносно невелика розрядність закритого ключа s меншого за q : $s < q$ відкриває можливості для його підбору. Суттєвою вадою методу є те, що цикл ідентифікації віддаленого користувача потребує трьох сеансів обміну даними між користувачем та системою, що помітним чином уповільнює процес ідентифікації.

Невирішені питання. На основі аналізу літературних джерел можна зробити наступні висновки. З теоретичної точки зору найбільш надійна ідентифікація віддаленого користувача досягається в рамках реалізації концепції "нульових знань".

Існуючі методи реалізації вказаної концепції мають за математичну основу аналітично нерозв'язну задачу дискретного логарифмування. Відповідно, базовими обчислювальними операціями для відомих методів виступають мультиплікативні операції модулярної арифметики. Для зменшення обчислювальної складності реалізації цих методів в відомих методах застосовано певні спрощення, зокрема використання операції модулярного піднесення до квадрату та чисел з меншою розрядністю. Ці спрощення компенсуються використанням декількох (від 3-х до 20) сеансів обміну даними між користувачем та системою, що суттєво уповільнює ідентифікацію користувачів.

В сучасних умовах практично всі сервери систем віддаленого надання користувачам доступу до інформаційних та обчислювальних ресурсів обладнані криптопроцесорами, які здатні з високою швидкістю виконувати мультиплікативні операції модулярної арифметики над числами, розрядність яких становить до 4096. Разом з тим, для обчислювальної платформи користувача, що не має криптопроцесора, час виконання мультиплікативних операцій модулярної арифметики суттєво впливає на швидкість ідентифікації. Таким чином, в сучасних умовах витрати часу на виконання обчислень на сервері системи, пов'язаних з процесом ідентифікації, стають менш критичним в порівнянні з часом, що витрачається на багатокроковий обмін даними. Відповідно, важливим резервом прискорення процесів ідентифікації користувачів в умовах багатократного зростання їх кількості є зменшення використання ліній передачі даних.

Мета дослідження полягає в прискоренні процедури криптографічно строгої ідентифікації віддалених користувачів в рамках концепції "нульових знань" за рахунок зменшення кількості сеансів обміну даними між системою та користувачем.

Для досягнення поставленої мети в роботі розв'язуються такі наукові задачі:

– розробка методу прискореної ідентифікації віддалених користувачів на основі теоретичної концепції "нульових знань";

– теоретичне та експериментальне дослідження ефективності методу прискореної ідентифікації віддалених користувачів, порівняльний аналіз показників його ефективності з відомими методами реалізації концепції "нульових знань".

2. Метод реалізації концепції "нульових знань" для ідентифікації віддалених користувачів. Для підвищення ефективності ідентифікації віддалених абонентів за рахунок зменшення кількості сеансів обміну інформацією між користувачем та системою пропонується метод ідентифікації, що має за математичну основу реалізації теоретичної концепції "нульових знань" незворотні перетворення теорії чисел.

В основі запропонованого методу ідентифікації віддалених користувачів покладено наступні теоретичні положення теорії чисел.

Якщо модуль M утворюється у вигляді добутку двох простих чисел p і q: $M=p \cdot q$, то функція Ейлера φ(M) визначається у вигляді $\varphi(M) = (p-1)\cdot(q-1)$. За умови, що найбільший спільний подільник (НСП) A та M дорівнює одиниці, тобто НСП(A,M)=1, то, згідно з узагальненням Ейлера малої теореми Ферма [4] : $A^{\varphi(M)} \bmod M = 1$. Наприклад, якщо p= 19,

а q = 13, то модуль $M=p\cdot q$ = 19·13 = 247, функція Ейлера $\varphi(M) = (p-1)\cdot(q-1)$ = 216 і для будь-якого A, що не ділиться на p=19 або q=13 $A^{216} \bmod 247 = 1$, зокрема $225^{216} \bmod 247 = 1$.

Розроблений метод, як і інші методи, передбачає процедури, що виконуються при реєстрації користувача в системі та процедури, що реалізуються безпосередньо в кожному циклі ідентифікації. Реєстрація користувача складається з наступної послідовності дій:

1) Користувач довільним чином вибирає два простих числа p і q. Бажано, щоб вибір пари простих p і q виконувався таким чином, щоб числа p-1 та q-1 мали якомога більше подільників. Формується модуль M як добуток вибраної пари простих чисел: $M=p\cdot q$. Обчислюється число $\varphi = (p-1)\cdot(q-1)$, що зберігаються користувачем в секреті. Зберігається також множина ϑ його можливих подільників.

2) По запиту користувача система пересилає йому свій відкритий закриваючий ключ $K_з$, який надає змогу шифрувати реєстраційні дані, що передаються в систему кожним із користувачів. В якості алгоритму несиметричного шифрування використовується алгоритм з відкритим ключем типу RSA. Відкриваючий ключ K_0 тримається системою в секреті.

3) Отримане значення модуля M шифрується відкритим ключем $K_з$ системи та пересилається в систему в якості відкритого ключа користувача.

4) З використанням секретного відкриваючого ключа K_0 система відновлює відіслане користувачем значення модуля M і зберігає його.

Передбачена розробленим методом процедура циклу ідентифікації полягає в виконанні наступної послідовності дій:

1) Користувачем генерується випадкове число A.

2) Виконується перевірка чи ділиться число A на p чи q . Якщо $A \bmod p = 0$ або $A \bmod q$, то перехід на повторне виконання п.1.

3) З використанням множини ϑ користувачем виконується розкладення числа φ на два співмножника v та w: $\varphi = v\cdot w$.

4) Виконується обчислення першої компоненти сеансового паролю $P = A^v \bmod M$. В якості другої компоненти сеансового пароля слугує число w.

5) Обидві компоненти сеансового паролю P та w шифруються системним відкритим ключем $K_З$ та відсилаються користувачем в систему.

6) Система з використанням закритого ключа K_0 розшифровує ідентифікуючую посилку користувача, відновлюючи обидві компоненти сеансового паролю P та w.

7) Система обчислює $Z = P^w \bmod M$ і порівнює отриманий результат з одиницею. Якщо Z = 1, то вважається, що ідентифікація користувача виконана успішно і останній отримує доступ до ресурсів системи.

Функціонування запропонованого методу може бути ілюстровано наступним прикладом. Згідно з описаною вище процедурою реєстрації, користувач довільним чином вибирає два простих числа p і q такі, щоб значення p-1 і q-1 мали якомога більше подільників. Наприклад, при виборі простого $p=19$ значення p-1=18 має чотири подільники 2, 3, 6 і 9, а при виборі простого q=17 значення q-1=16 має три подільники: 2, 4, 8. Обчислюється число $\varphi = (p-1)\cdot(q-1) = 18\cdot16 = 288$, що зберігається в секреті. Зберігається також множина ϑ його можливих подільників.

Користувач обчислює значення модуля $M=p\cdot q$ = 19·17 = 323. Обчислене значення в зашифрованому вигляді пересилається в систему і являє собою відкритий ключ користувача.

Для виконання циклу ідентифікації користувач, згідно п.1 описаної процедури генерує випадкове число, наприклад, A= 255. В рамках п.2 виконується перевірка того, що вибране число не ділиться на одне з чисел p і q. Оскільки $255 \bmod 19 = 8 \neq 0$ але $255 \bmod 17 = 0$, тобто згенероване число A ділиться на q=17, то реалізується перехід на повторне виконання п.1. При повторному виконанні п.1 користувач генерує випадкове число A= 100 Наступним п.2 виконується перевірка $100 \bmod 19 = 5 \neq 0$ або $100 \bmod 17 = 15 \neq 0$.

В рамках п.3 запропонованої процедури користувачем виконується розкладення числа φ=288 на два співмножника v та w: наприклад v=32 та w=9. Виконується обчислення першої компоненти сеансового паролю $P = A^v \bmod M = 100^{32} \bmod 323 = 256$. Друга компонента

сеансового паролю w=9. Пара чисел P = 256 та w=9 шифруються відкритим системним ключем $К_3$ та передаються в систему. Остання розшифровує отримане повідомлення з використанням закритого ключа $К_0$, відновлюючи значення P = 256 та w=9. У відповідності до п.7 описаної вище процедури ідентифікації система обчислює значення $Z = P^w \bmod M$ $Z = 256^9 \bmod M$ 323 = 1. В силу того, що обчислене значення Z дорівнює одиниці, що підтверджує ідентичність користувача. ідентифікація вважається виконаною успішно.

3. Аналіз ефективності. Основними показниками ефективності процедури ідентифікації, як і будь-якого механізму криптографічного захисту інформації, є рівень захищеності та швидкість реалізації функцій захисту.

В теоретичному плані запропонований метод ідентифікації віддалених користувачів цілком відповідає концепції “нульових знань” в силу того, що:

– сеансові паролі змінюються в кожному циклі ідентифікації;

– системі надано механізм перевірки правильності сеансових паролів користувачів, проте сама система не може генерувати такі паролі.

Для того, щоб система могла генерувати коректний сеансовий пароль у вигляді пари чисел P та w таких, щоб $P^w \bmod M$ =1 їй потрібно фактично відновити значення простих співмножників модуля M – простих чисел p та q, таких, що $M = p \cdot q$. Це класична задача [5] розкладення числа на прості співмножники, Вирішення такої задачі при розрядностях M більших за 1024, потребує ресурсів, об’єм яких в переважній більшості випадків виходить за рамки практичної доцільності навіть при використанні сучасних хмарних технологій [6].

Таким чином, при використанні запропонованого методу, система практично не здатна генерувати коректний сенсів пароль користувача. Відповідно, виключається можливість імітації звернення користувача до системи та використання інформації. що міститься в системі для генерації коректних сеансових паролів користувачів.

Для сторони, яка здійснює пасивний чи активний доступ до каналу передачі даних, підбір коректного сеансового пароля ускладнюється тим, що їй не відомий модуль M. Відповідно, для цієї сторони задача отримання незаконного доступу до ресурсів системи за рахунок підробки сеансових паролей користувачів практично не може бути реалізована.

Основна перевага розробленого методу ідентифікації віддалених користувачів полягає в використанні лише одного використання каналу передачі даних між системою та абонентом. Це дозволяє в сучасних умовах суттєво прискорити виконання процедури ідентифікації в порівнянні з відомими методами. Фактично, час потрібний на виконання ідентифікації визначається двома складовими: часом на реалізацію передбачених методом обчислень та часом, потрібним для обміну ідентифікаційною інформацію між системою та користувачем.

Десять років тому, коли широкого розповсюдження набуло використання методів ідентифікації на основі прогресивної концепції “нульових знань” кількість користувачів ще не була такою значною як нині, а для реалізації мультиплікативних операцій над числами великої розрядності використовувалися безпосередньо універсальні процесори, часова складова, пов’язана з реалізацією обчислень переважала [7].

В сучасних умовах динамічного розвитку хмарних технологій і, відповідно, лавиноподібного зростання кількості користувачів інтегрованих систем надання інформаційних та обчислювальних ресурсів, питома вага часової складової пов’язаною з обміном даними має тенденцію до зростання. Основні чинники цього полягають в зростанні кількості користувачів, звернення яких до системи носить випадковий характер. Разом з тим, практично всі сучасні сервери обладнані спеціалізованими криптопроцесорами, які здатні швидко реалізувати операції модулярного експоненціювання над числами розрядністю 1024, 2048 та 4096. Зокрема, криптопроцесор моделі 6500 американської фірми Hi/fn виконує операцію модулярного експоненціювання за десятки наносекунд. Це має наслідком значне зменшення питомої ваги часових затрат на ідентифікацію, пов’язаних з виконанням відповідних обчислень.

В запропонованому методі найбільш ресурсоємні операції модулярного експоненціювання виконуються як користувачем так і системою. Остання реально виконує ці операції на криптопроцесорі сервера системи і, відповідно, їх виконання не займає багато часу. Проте, в переважній своїй більшості, обчислювальні платформи користувачів не обладнані спеціалізованими криптопроцесорами. Відповідно, виконання операцій, передбачених п.3 та п.4 наведеної вище процедури ідентифікації займають доволі багато часу. Проте, як видно з наведеної процедури, вказані операції можуть виконуватися заздалегідь і час їх виконання прямо не впливає на швидкість ідентифікації користувача.

Таким чином, використання в розробленому методі однієї пересилки надало змогу фактично виключити з сумарного часу ідентифікації час, потрібний на обчислення, що виконує користувач. Саме ця відмінність запропонованого методу, як показали результати експериментальних досліджень, суттєвим чином впливає на час ідентифікації.

Для аналізу ефективності запропонованого методу в плані прискорення процесу ідентифікації в рамках теоретичної концепції нульових знань було проведено спеціальні експериментальні дослідження з реальним використанням мережі Інтернет. Отримані результати порівняльного аналізу швидкодії запропонованого методу ідентифікації та ряду відомих методів, що також реалізують теоретичну концепцію “нульових знань” наведені в табл. 1.

Табл. 1

Відомий метод	Прискорення виконання циклу ідентифікації при використанні розробленого методу для розрядностей чисел 1024 і 2048	
	1024	2048
FESIS	8.24	7.93
Guillou-Quisquater	2.43	1.87
Schnorr	1.96	1.64

Проведені експериментальні дослідження показали, що розроблений метод ідентифікації віддалених користувачів за рахунок використання лише одного сеансу обміну даними між користувачем дозволяє помітним чином прискорити процес ідентифікації, забезпечуючи при цьому високий рівень захищеності.

4. Висновки. В результаті проведених досліджень розроблено метод, що реалізує теоретичну концепцію “нульових знань” строгої ідентифікації віддалених користувачів інтегрованих систем надання інформаційних та обчислювальних ресурсів. Відмінність запропонованого методу полягає з використанням одного сеансу обміну даними між системою та користувачем, що дозволяє прискорити процес його ідентифікації. Математичною основою запропонованого методу є використання незворотних перетворень теорії чисел. Метод безпосередньо базується на властивостях узагальнення Ейлера малої теореми Ферма.

Проведений теоретичний аналіз рівня захищеності від спроб незаконного проникнення до ресурсів системи, що забезпечує запропонований метод, показав, тотожність задачі порушення захисту математичним задачам, розв’язання яких потребує обчислювальних ресурсів, об’єм яких знаходиться за межами практичної доцільності. Проведеними експериментальними дослідженнями показано, що розроблений метод забезпечує прискорення процесу ідентифікації віддалених користувачів в порівнянні з відомими методами, що базуються на теоретичній концепції “нульових знань”.

Список використаної літератури

1. Feige U. Zero knowledge proofs of identity / U. Feige., A. Fiat., A. Shamir // Journal of Cryptology. – 1988. – Vol. 1, №.2. – PP. 77-94.

2. Bengio S. Secure implementation of identification system / S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, J. J. Quisquater // Juornal of Cryptology. – 1991. – Vol. 4, №3. – PP. 186-192.

3. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. / B. Schneier. – Ed. John Wiley, 1996. – 758 p.

4. Харин Ю. С. Математические и компьютерные основы криптологии / Ю С. Харин., В. И. Берник., Г В. Матвеев, С. В. Агиевич. – Минск: Изд-во Новое знание, 2003. – 383 с.

5. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – Москва : Постмаркет, 2001. – 323 с.

6. Молдовян А. А. Введение в криптосистемы с открытым ключом / А. А. Молдовян, Н. А. Молдовян. С-Пб.: БХВ-Петербург,- 2004.-322 с.

7. Марковський О. П. Один підхід до прискорення строгої ідентифікації віддалених абонентів / О. П. Марковський, І. В. Ткач, Д. Г. Іванов. // Харківський університет Повітряних Сил імені Івана Кожедуба. Системи обробки інформації. Проблеми і перспективи розвитку ІТ-індустрії. – 2012. – Випуск 8(106). – С. 111-115.

References

1. Feige U., Fiat A., Shamir A. Zero knowledge proofs of identity // Journal of Cryptology. – 1988. – Vol.1, №.2. – PP.77-94.

2. Bengio S., Bengio S., Brassard G., Desmedt Y. G., Goutier C., Quisquater J. J. Secure implementation of identification system // Jornal of Cryptology. – 1991. – Vol.4, №3. – PP.186-192.

3. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. – Ed.John Wiley, 1996. – 758 p.

4. Kharin Yu. S., Bernik V. I., Matveev G. V., Agievich S. V. Mathematical and computer bases of cryptology. – Minsk : Novoye znaniye, 2003. –383 p.

5. Koutikho S. Introduction to the numbers theory. RSA Algorithm. Moskva : Postmarket. – 2001. – 323 p.

6. Moldovyan A. A., Moldovyan N. A. Introduction to the opened key cryptocyctems. – Sankt-Peterburg: BKhV-Peterburg, 2004. – 322 p.

7. Markovskyi O. P., Tkach I. V., Ivanov D. H. Methodof the fast strict identification of the distant subscribers // Ivan Kozhedub Khakiv Univercity of Aircrafts. Systems of information treatment. Problems and prospects of IT-industry development. – 2012. – No. 8(106). – PP. 111-115.

Автори статті

Мухін Вадим Євгенійович – доктор технічних наук, професор кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут» імені Ігора Сікорського, Київ. Тел.: +380 (67) 508 76 84. E-mail: v_mukhin@mail.ru

Захаріудакіс Лефтерис – аспірант кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут» імені Ігора Сікорського, Київ. Тел.: +380 (97) 799 24 62. E-mail: 5b4agl@gmail.com

Герасименко Оксана Юріївна – асистент кафедри мережевих та інтернет технологій, Київський національний університет імені Тараса Шевченка, Київ. Тел.: +380 (99) 785 87 58. E-mail: oksgerasymenko@gmail.com

Козерацький Михайло Сергійович – аспірант кафедри прикладної гідроаеромеханіки та механотроніки Національний технічний університет України «Київський політехнічний інститут» імені Ігоря Сікорського, Київ. Тел.: +380 (50) 730 10 27. E-mail: kozeratskiy@i.ua

Authors of the article

Mukhin Vadym Yevheniiovych – doctor of sciences (technic), professor of computer systems department, Ihor Sikorsky National Technical University of Ukraine “Kiev Polytechnic Institute”, Kyiv. Tel.: +380 (67) 508 76 84. E-mail: v_mukhin@mail.ru

Zahariudakis Lefteris – PhD student of computer systems department, Ihor Sikorsky National Technical University of Ukraine “Kiev Polytechnic Institute”, Kyiv. Tel.: +380 (97) 799 24 62. E-mail: 5b4agl@gmail.co

Herasymenko Oksana Yuriivna – assist. professor of networking and internet technologies department, Taras Shevchenko National University, Kyiv. Tel.: +380 (99) 785 87 58. E-mail: oksgerasymenko@gmail.com

Kozeratskiy Mykhailo Serhiiovych – PhD student of applied fluid mechanics and mechatronics department, Ihor Sikorsky National Technical University of Ukraine “Kiev Polytechnic Institute”, Kyiv. Tel.: +380 (50) 730 10 27. E-mail: kozeratskiy@i.ua

Дата надходження в редакцію:
27.12.2016 р.

Рецензент:
доктор технічних наук, професор О. А. Стенін
Національний технічний університет України
«Київський політехнічний інститут» ім. Ігора Сікорського