материал, развить свои способности в решении проблемы защиты информации, разбираться в тех или иных вопросах информационной безопасности и учиться работать в коллективе. Деловые игры помогут обеспечить будущих специалистов по информационной безопасности необходимыми теоретическими знаниями и практическими навыками в сфере современных методов и средств защиты информации.
Ключевые слова: информационная безопасность; модель высшего профессионального образования; техническая защита; деловые игры; профессиональная подготовка.

BUSINESS GAMES AS A METHOD OF TRAINING INFORMATION SECURITY SPECIALISTS

Providing an adequate level of information security is directly dependent on quality training of future specialists, the level of implementation and use of innovative teaching, infocommunication technologies and information culture. The current state of training specialists of information security industry indicates that the current requirements for skills and experience of students do not consistent with are necessary for building an effective information security management system of the organization. The paper disclosed methodology of business games for training specialists in information security industry. The described method of training will allow students better understand the material, develop their ability in solving the problem of information security, understand some or other questions of information security, and learn to work in teams. The business games help to ensure the future information security professionals necessary theoretical knowledge and practical skills in modern methods and tools of information security.
Index Terms: information security; model of higher education, technical protection, business games, training.

Шиліна Наталія Євгеніївна, кандидат педагогічних наук, доцент, Одеська національна академія зв'язку ім. О.С. Попова.
E-mail: natuccy@mail.ru
Шилина Наталия Евгениевна, кандидат педагогических наук, доцент, Одесская национальная академия связи им. А.С. Попова.
Shylina Nataliia, PhD, associate professor, Odessa National Academy of Telecommunications named after O.S.Popov.

Копитін Юрій Вікторович, комунальне підприємство «Обласний інформаційно-аналітичний центр», т.в.о. начальника відділу забезпечення захисту інформації, Одеська національна академія зв'язку.
E-mail: ykopitin@odessa.gov.ua
Копытин Юрий Викторович, коммунальное предприятие "Областной информационно-аналитический центр", и.о. начальника отдела защиты информации, Одесская национальная академия связи им. А.С. Попова.
Kopytin Yuriy, municipal enterprise "Regional information-analytical center", the acting head of the department of information security, Odessa National Academy of Telecommunications named after O.S.Popov.

УДК 621.391.7

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ ДЛЯ ЗДІЙСНЕННЯ АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрий Яремчук

В роботі розглянуто математичний апарат рекурентних V_k^+ *та* U_k *– послідовностей, а також можливість побудови методу автентифікації сторін взаємодії на його основі. Для запропонованого методу розроблено принципи побудови спеціалізованих процесорів для можливості доведення та перевірки автентичності відповідно кожною із сторін взаємодії. Порівняння швидкості роботи розроблених процесорів з відомими аналогами показало, що за певних умов час роботи розроблених спеціалізованих процесорів автентифікації буде в десятки разів меншим, ніж на процесорах, що реалізують відомі методи. Розроблені спеціалізовані процесори мають перспективи використання в задачах різного криптографічного призначення, що базуються на технології відкритого ключа.*
***Ключові слова**: спеціалізовані процесори, захист інформації, криптографія, автентифікація, рекурентні послідовності.*

Вступ. На сьогодні задача забезпечення цілісності інформації є не менш, а в деяких випадках і більш актуальною, ніж задача конфіденційності інформації. Для забезпечення цілісності розробляються криптографічні протоколи [1-6], найбільш розповсюдженими з яких є два типи протоколів – автентифікації та цифрового підписування. Що стосується автентифікації, то в основ-

ному 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 [4] 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 [7]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1, 2, 4, 5]. 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. В роботі [8] представлено метод автентифікації сторін взаємодії, який базується на рекурентних V_k^+ та U_k –послідовностях і який, у порівнянні з відомим методами, усуває вказані труднощі, дозволяючи суттєво спростити обчислення.

Особливість криптографічних методів полягає в тому, що в них необхідно виконувати обчислення над числами великої розрядності (1024–4096 двійкових розрядів), що вимагає великого часу і тому програмна реалізація не завжди є прийнятною. Підвищення швидкості криптографічних перетворень може бути досягнуто за рахунок їх апаратної реалізації. Тому розглядається можливість побудови спеціалізованих процесорів для здійснення автентифікації сторін взаємодії на основі рекурентних V_k^+ та U_k –послідовностей.

Постановка задач досліджень. Розглянути математичний апарат рекурентних V_k^+ та U_k –послідовностей з можливістю побудови швидкісного методу автентифікації сторін взаємодії та розробити принципи побудови спеціалізованих процесорів на їх основі. Дослідити запропоновані процесори щодо швидкості їх роботи і порівняти з відповідними процесорами, що реалізують відомі методи-аналоги.

Автентифікація сторін взаємодії на основі рекурентних послідовностей

V_k^+ –послідовністю [9] називається 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 $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

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

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

U_k –послідовністю [9] називається послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \quad (3)$$

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.

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

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

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

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} \cdot \quad (5)$$

Метод автентифікації сторін взаємодії [8] базується на властивості (4), яка дозволяє обчислити елемент $u_{n+m,k}$, використовуючи елементи V_k^+ та U_k –послідовностей, причому зробити це 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 вигляд, що представлено на рис.1.

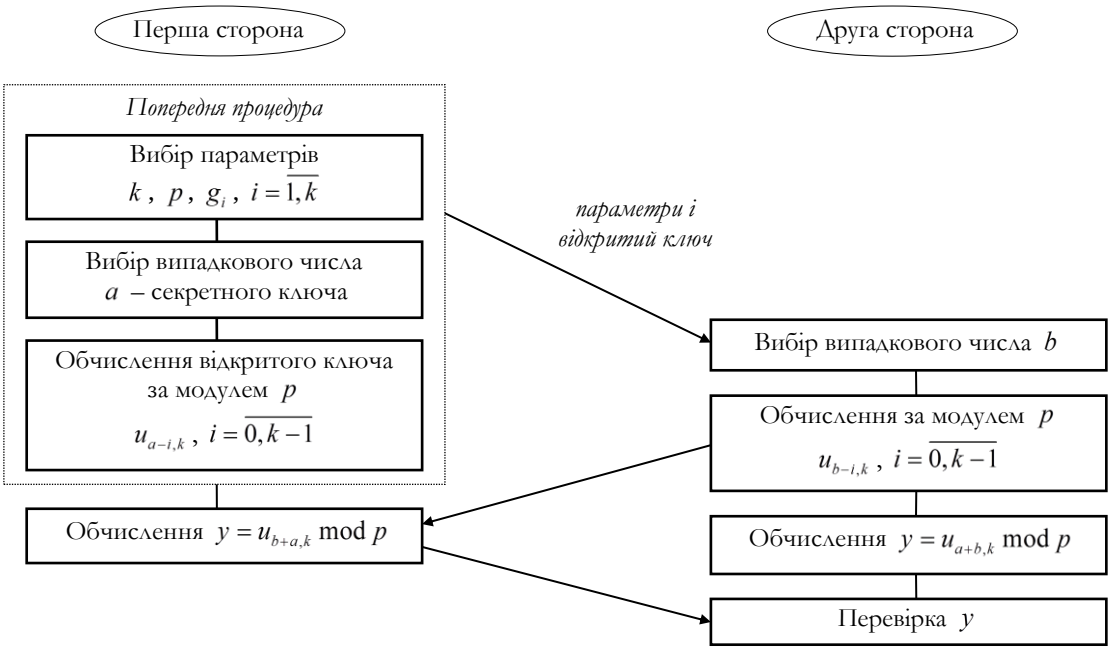

Рис. 1. Схема автентифікації сторін взаємодії на основі елементів U_k - послідовності.

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

Відповідно до запропонованого методу основні обчислення виконуються згідно залежності (4). 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 (5), 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 (4) 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.

Проблема обчислення елементу $v_{n,k}$ полягає в тому, що для великих значень n, а саме такі значення повинні використовуватись в криптографічних перетвореннях, обчислення $v_{n,k}$ за формулою (1) є неприйнятним. Тому обчислення елементу $v_{n,k}$ може здійснюватись за алгоритмом прискореного обчислення елементів V_k^+ - послідовності [9], що реалізований на основі відомого бінарного методу піднесення до степеня [2].

Слід відзначити, що розглянутий метод автентифікації сторін взаємодії на основі елементів U_k -послідовності ще не забезпечує усім вимогам, які висуваються до протоколів автентифікації,

оскільки не дозволяє використовувати сеансовий ключ з боку Першої сторони, що доводить свою автентичність. Однак і в такому представленні метод може використовуватись в певних застосуваннях.

Розробка принципів побудови спеціалізованих процесорів для здійснення автентифікації сторін взаємодії. Для реалізації представленого методу автентифікації сторін взаємодії необхідні процедури для обчислення за модулем p елементів $v_{n+i,k}$, $i=\overline{-(k-1),k-2}$, а також елементів $u_{n-i,k}$, $i=\overline{0,k-1}$, та $u_{n+m,k}$. Всі ці обчислення пропонується здійснювати на одному універсальному пристрої обчислення елементів V_k^+ – та U_k –послідовностей, роботу якого організуємо в п'яти режимах. В першому режимі будемо здійснювати обчислення елементів $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$, для додатних значень n, а в другому - обчислення елементів $v_{n+i,k}$, $i=\overline{-k,k-2}$, для від'ємних значень n. Третій, четвертий та п'ятий режими роботи пристрою будуть забезпечувати відповідно обчислення елементів $u_{n-i,k}$, $i=\overline{0,k-1}$, за формулою (5), $u_{n+m-i,k}$, $i=\overline{0,k-1}$, за формулою (4) та $u_{n-m-i,k}$, $i=\overline{0,k-1}$.

Для реалізації обчислень Першою стороною, яка повинна довести свою автентичність, згідно представленого методу пропонується процесор, схему якого наведено на рис. 2.

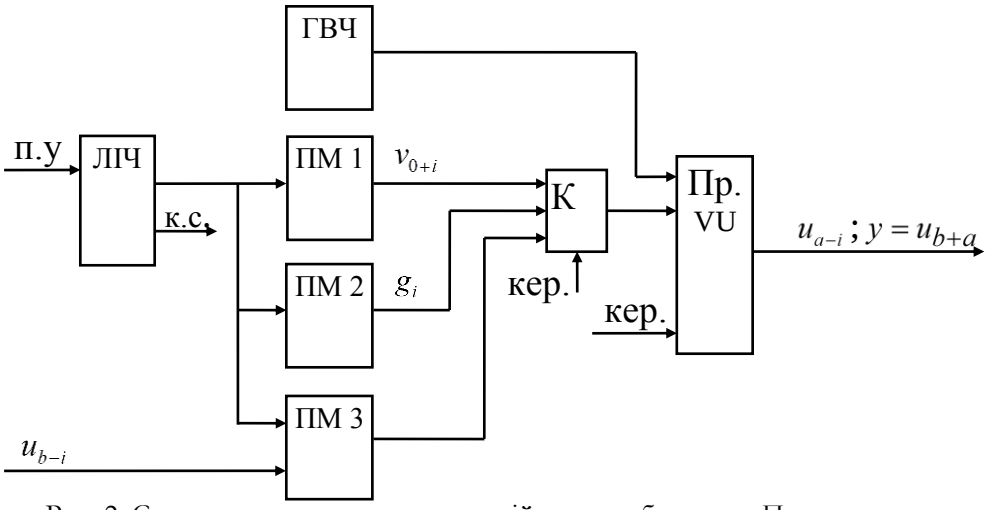

Рис. 2. Структурна схема процесора здійснення обчислень Першою стороною щодо доведення своєї автентичності

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k^+ – та U_k –послідовностей Пр.VU; блоки пам'яті ПМ 1, ПМ 2, призначені для зберігання відповідно елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, та коефіцієнтів рекурентної залежності g_i, $i=\overline{1,k}$; блок пам'яті ПМ 3, призначений для зберігання Першою стороною елементів $u_{b-i,k}$, $i=\overline{0,k-1}$, що отримуються від Другої сторони; комутатор К; лічильник ЛІЧ.

Доведення своєї автеничності Першою стороною здійснюється таким чином.

Генератор ГВЧ генерує випадкове число a, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1, подаються на відповідні входи пристрою Пр.VU, після чого здійснюється робота цього пристрою в першому режимі, коли обчислюються елементи $v_{a+i,k}$, $i=\overline{-2k+1,k-2}$. Далі на вхід пристрою Пр.VU подаються дані з блоку пам'яті ПМ 2 і в третьому режимі обчислюються за модулем p елементи $u_{a-i,k}$, $i=\overline{0,k-1}$, які передаються Другій стороні.

Потім з блоку пам'яті ПМ 3 на вхід пристрою Пр.VU подаються елементи $u_{b-i,k}$, $i=\overline{0,k-1}$, прийняті від Другої сторони і в четвертому режимі роботи пристрою Пр.VU обчислюється елемент $u_{b+a,k}$ за модулем p як результат коду для перевірки автентичності y, який передається Другій стороні.

Не важко помітити, що процесор для реалізації обчислень Другою стороною, яка перевіряє автентичність Першої сторони, має бути в осно-

вному аналогічним тому, що і для обчислень Першою стороною. Відмінність полягає лише в тому, що Другій стороні необхідно перевірити обчислене значення y як результат $u_{b+a,k}$ за модулем p з отриманим значенням y від Першої сторони шляхом віднімання і пересвідченням того, що отриманий результат буде нулем. Для цього до процесору перевірки автентичності слід ввести додатковий блок пам'яті ПМ 4 для зберігання прийнятого від Першої сторони значення $y = u_{b+a,k} \bmod p$, а також ввести пристрій віднімач ВДЧ для перевірки цього значення з обчисленим значенням $y = u_{a+b,k} \bmod p$.

Також слід зазначити, що обчислення за модулем p елементів $u_{b-i,k}$, $i = \overline{0,k-1}$, буде здійснюватись щоразу при кожному сеансі автентифікації сторін, в той час як відкритий ключ $u_{a-i,k}$, $i = \overline{0,k-1}$, буде обчислюватись за модулем p Першою стороною лише один раз перед великою серією таких сеансів.

Враховуючи вищесказане, процесор для реалізації обчислень Другою стороною згідно представленого методу буде мати вигляд, схему якого наведено на рис. 3.

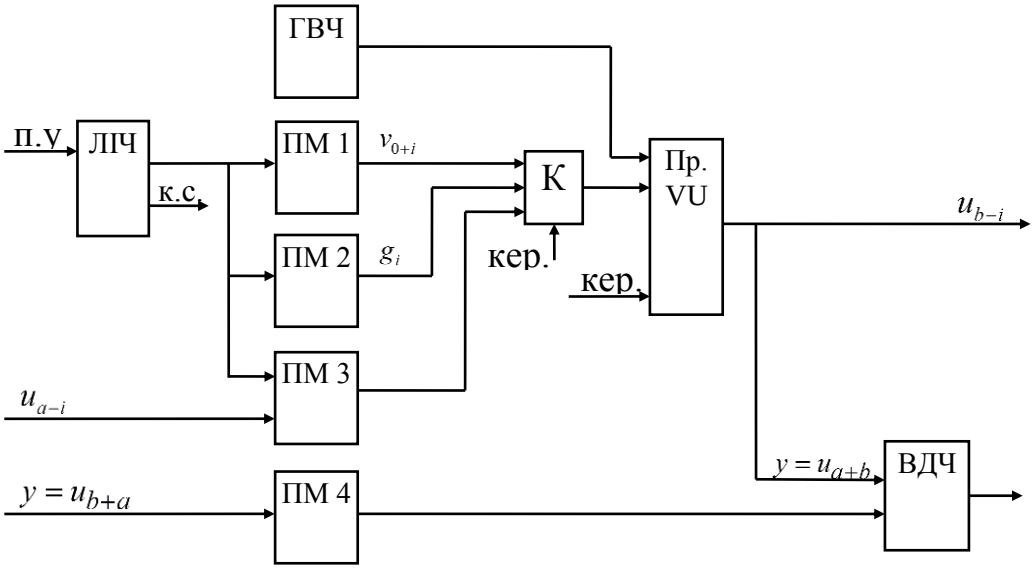

Рис. 3. Структурна схема процесора здійснення обчислень Другою стороною щодо перевірки автентичності Першої сторони

Після отримання Другою стороною коду для перевірки автентичності y від Першої сторони процесор перевірки автентичності обчислює елемент $y = u_{a+b,k} \bmod p$ під час роботи пристрою Пр.VU в четвертому режимі, та перевіряє його із значенням $y = u_{b+a,k} \bmod p$, що знаходиться в блоці памяті ПМ 4, за допомогою пристрою віднімача ВДЧ. Якщо на виході віднімача ВДЧ буде нуль, то автентичність Першої сторони буде вважатись підтвердженою.

Проведемо тепер дослідження часу роботи розроблених процесорів та порівняємо їх з часом роботи процесорів, що реалізують відомі аналоги.

В результаті дослідження встановлено, що час обчислення елементів V_k^+-послідовності в першому і другому режимах його роботи дорівнює: $T_V = Hq \cdot \left(k^2 + k\right) \cdot T_{мн.Монт.}$, де H – кількість машинних одиниць інформації для зберігання великого числа, q – кількість розрядів машинної одиниці інформації, $T_{мн.Монт.}$ – час множення за модулем за методом Монтгомері, а час обчислення елементів U_k-послідовності в третьому, четвертому і п'ятому режимах дорівнює: $T_U = \left(k^2 + k\right) \cdot T_{мн.Монт.}$.

Оскільки в сучасних криптосистемах оперують з числами 1024 або 4096 розрядів, тобто Hq приймає саме такі значення, то оцінкою обчислення елементів $u_{n,k}$ можна знехтувати. Враховуючи це, в цілому час обчислень як Першою стороною так і Другою стороною на процесорах, що представлені відповідно на рис. 2 та 3, буде дорівнювати $T = Hq \cdot \left(k^2 + k\right) \cdot T_{мн.Монт}$.

Проведемо тепер порівняння розроблених процесорів автентифікації сторін взаємодії з від-

повідними спеціалізованими процесорами, що реалізують відомі методи.

Основною операцією, що виконується у відомих методах Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра є піднесення до степеня за модулем. Ця операція може здійснюватись за методом Монтгомері [2], який має меншу складність обчислень, ніж відомий бінарний метод [2]. Метод піднесення до степеня за Монтгомері оснований на множенні за методом Монтгомері. Виходячи з цього, пристрій піднесення до степеня за Монтгомері можна побудувати на основі пристрою множення за Монтгомері, який використовується в процесорах, що реалізують представлений метод автентифікації сторін взаємодії.

Час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати $T_{ПДС\bmod} = 2(Hq+1)\cdot T_{мн.Монт.}$

За основу порівняння візьмемо аналог – відомий метод Шнорра, в який вимагає чотирьох піднесень до степеня за модулем – по два з боку кожної сторони, причому сторона, яка доводить свою автентичність, одне піднесення до степеня виконує в попередній процедурі визначення параметрів та ключів і одне підчас безпосередньої автентифікації, при цьому сторона, що перевіряє автентичність, виконує два піднесення до степеня за модулем тільки безпосередньо підчас самої автентифікації.

Таким чином, використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесору для автентифікації сторін взаємодії за відомим методом Шнорра, отримаємо час виконання операцій на цьому процесорі як з боку однієї сторони в цілому так і з боку другої сторони $T_{Шнорра} = 4(Hq+1)\cdot T_{мн.Монт.}$.

Аналіз отриманих оцінок показує, що час доведення автентичності в цілому з боку Першої сторони так і час перевірки з боку Другої сторони на процесорах, що реалізують відомий метод Шнорра, є меншим, ніж на процесорах, що реалізують представлений метод відповідно кожною стороною на основі рекурентних V_k^+ – та U_k – послідовностей, причому більше ніж у 1,5 рази, навіть для $k=2$.

Однак тут слід враховувати таке. Обчислення елементів $u_{a-i,k}$, $i=\overline{0,k-1}$, згідно залежності (5), а отже і елементів $v_{a+i,k}$, $i=\overline{-2k+1,-1}$, які необхідні для цих обчислень, здійснюється в попередній процедурі визначення ключів та вибору параметрів. Тобто ці обчислення здійснюються один раз перед безпосередніми сеансами автентифікації. Так само і обчислення елементів $u_{b-i,k}$, $i=\overline{0,k-1}$, згідно залежності (5) та необхідних для цього елементів $v_{b+i,k}$, $i=\overline{-2k+1,-1}$, також можна здійснювати заздалегідь і зберігатись в блоці пам'яті пристрою Пр.VU до безпосереднього початку процесу перевірки автентичності.

Враховуючи це, час роботи запропонованих процесорів буде значно меншим, на порядки меншим, оскільки за таких умов обчислення будуть проводитись лише за формулою (4) елементу $u_{b+a,k}$ або $u_{a+b,k}$, тобто час роботи буде дорівнювати лише приблизно $2(k-1)\cdot T_{мн.Монт.}$, що в декілька десятків разів менше, ніж за відомим методом Шнорра, коли необхідно виконувати піднесення до степеня великого числа і час роботи кожного з процесорів в цьому випадку буде дорівнювати $2(Hq+1)\cdot T_{мн.Монт.}$.

Висновки. Розглянуто математичний апарат рекурентних V_k^+ – та U_k –послідовностей. На основі цього апарату представлено метод автентифікації сторін взаємодії, який хоч і не задовольняє усім вимогам до протоколів автентифікації, оскільки не дозволяє використовувати сеансовий ключ з боку сторони, що доводить свою автентичність, однак і в такому представленні може мати доволі широке застосування.

Розроблено спеціалізовані процесори, які реалізують представлений метод автентифікації з боку кожної сторони взаємодії.

Проведено дослідження часу роботи розроблених процесорів. Дослідження показало, що з врахуванням можливості виконання заздалегідь попередніх процедур обчислення відкритого ключа стороною, що доводить автентичність, та обчислення елементів U_k –послідовності на основі сеансового ключа стороною, що перевіряє автентичніть, час роботи розроблених спеціалізованих процесорів автентифікації буде в десятки разів меншим, ніж на процесорах, що реалізують відомі методи, зокрема метод Шнорра.

ЛІТЕРАТУРА

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

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

[3]. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – М: Гелиос АРВ, 2001. – 480 с.
[4]. Введение в криптографию / Под общ. ред. В.Б. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 236 с.
[5]. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
[6]. Брассар Ж. Современная криптология. – М.: ПОЛИМЕД, 1999. – 176 с.
[7]. Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411-431.
[8]. Яремчук Ю.Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – №1, 2013. – С. 4–10.
[9]. Яремчук Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. – №4, 2012. – С. 120–127.

REFERENCES

[1]. Romanets Yu.V., Timofeeva P.A., Shangin V.F. Information protection in computer systems and networks, M.: Radio and communication, 2001, 376 p.
[2]. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography, CRC Press, 2001, 816 p.
[3]. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Foundations of cryptography, M: Helios ARV, 2001, 480 p.
[4]. Introduction to Cryptography / Ed. red. V.B. Yaschenko. - M: MCCME "CheRo", 2000, 236 p.
[5]. Petrov A.A. Computer Security. Cryptographic protection methods. - M.: DMK, 2000, 448 p.
[6]. Brassard J. Modern cryptology. - M: Polimed, 1999 , 176 p.
[7]. Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411-431.
[8]. Yaremchuk Yu.Ye. Authentication Method party interaction based on recurrent sequences /Suchasnyy zahist informatsii, № 1, 2013, P. 4-10.
[9]. Yaremchuk Yu.Ye. Using recursive sequences for constructing cryptographic techniques with public key / Information Security, № 4, 2012, P. 120-127.

СПЕЦИАЛИЗИРОВАННЫЕ ПРОЦЕССОРЫ ДЛЯ ОСУЩЕСТВЛЕНИЯ АУТЕНТИФИКАЦИИ СТОРОН ВЗАИМОДЕЙСТВИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В работе рассмотрен математический аппарат рекуррентных V_k^+ и U_k – последовательностей, а также возможность построения метода аутентификации сторон взаимодействия на его основе. Для предложенного метода разработаны принципы построения специализированных процессоров для возможности доказательства и проверки аутентичности соответственно каждой из сторон взаимодействия. Сравнение скорости работы разработанных процессоров с известными аналогами показало, что при определённых условиях время работы разработанных специализированных процессоров аутентификации будет в десятки раз меньше, чем на процессорах, реализующих известные методы. Разработанные специализированные процессоры имеют перспективы использования в задачах различного криптографического назначения, в основе которых лежит технология открытого ключа.
Ключевые слова: специализированные процессоры, защита информации, криптография, аутентификация, рекуррентные последовательности.

SPECIALIZED PROCESSORS FOR AUTHENTICATION OF THE INTERACTION PARTIES BASED ON RECURRENT SEQUENCES

In this work, we consider the mathematical apparatus of recurrent V_k^+ and U_k sequences, as well as a possibility of constructing an authentication method for the parties, based on it. For the proposed method, we developed principles of specialized processors with a possibility for each party of interaction to prove and validate the authenticity. Comparison of the speed of the developed processors with the known analogues showed that, under certain conditions, the work time of the developed specialized authentication processors will be dozens of times less than the processors implementing the known methods. The developed specialized processors have a perspective to be used in various cryptographic tasks, based on the public key technology.
Keywords: specialized processors, information security, cryptography, authentication, recurrent sequence

Яремчук Юрій Євгенович, кандидат технічних наук, доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри адміністративного та інформаційного менеджменту Вінницького національного технічного університету.
E-mail: yurevyar@vntu.net
Яремчук Юрий Евгеньевич, кандидат технических наук, директор Центра информационных технологий и защиты информации, професор кафедри административного и информационного менеджмента Винницкого национального технического университета
Yaremchuk Yuriy, Phd, Director of the Center for Information Technology and Information Security, professor Department of Administrative and Information Management VNTU