2 Забезпечення комп'ютерної безпеки в інформаційних системах

Юрій Яремчук
Вінницький національний технічний університет
УДК 681.3.067

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ МЕТОДУ АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Анотація: **Проведено дослідження статистичної безпеки методу автентифікації сторін взаємодії на основі рекурентних V_k –послідовностей та здійснено його порівняння з відомими методами Шнорра, Фіата-Шаміра та Фейге-Фіата-Шаміра. Результати аналізу показали, що в цілому метод на основі V_k –послідовностей має стабільно високі показники, характеризуючи його з кращого боку щодо статистичної безпеки. Особливо це стосуються для малих довжинах ключів, що, в першу чергу, рекомендує його застосування в системах автентифікації, для яких використання великих ключів не є важливим.**
Summary: **The research are conducted for statistical security of the method of authentication the parties interaction based on recurrent V_k sequences and made his comparison with well-known Schnorr, Fiat-Shamir and Feige-Fiat-Shamir methods. Results of analysis showed that the overall method based on V_k sequences has consistently high scores, characterizing his best side on the statistical security. This is especially concerning for small lengths of keys that, first and foremost, recommends its use in authentication systems, which use large keys is not important.**
Ключові слова: **Криптографія, автентифікація, криптостійкість, статистична безпека, рекурентні послідовності**

I Вступ

Автентифікація сторін взаємодії – це процес криптографічних перетворень, під час якого одна зі сторін переконується в ідентичності другої сторони, а також в тому, що друга сторона активна у часі або безпосередньо перед моментом підтвердження доказів [1, 2]. В процесі автентифікації беруть участь дві сторони: претендент (claimant) та перевіряльник (verifier). Розрізняють парольну автентифікацію, автентифікацію за типом запит-відповідь (challenge–response), а також автентифікацію на основі доведення з нульовим розголошенням [1]. Остання полягає в тому, що претендент як санкціонований користувач, який має секретний та відкритий ключ, та перевіряльник спільно здійснюють інтерактивне доведення шляхом криптографічних перетворень, під час якого претендент повинен довести свою справжність, продемонструвавши знання секретного ключа законного користувача, але не розголошуючи його для перевіряльника, тобто з інформації, отриманої перевіряльником, йому обчислювально неможливо отримати секретний ключ претендента.

Серед існуючих методів автентифікації сторін взаємодії з нульовим розголошенням найбільш відомими є методи Фіата-Шаміра [3], Фейге-Фіата-Шаміра [4], Гіллоу-Куіскуотера [5] та Шнорра [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 актуальним залишається підвищення стійкості схем автентифікації.

В цьому зв'язку певний інтерес викликають методи автентифікації сторін взаємодії [7–10], що базуються на математичному апараті рекурентних U_k – та V_k –послідовностей. Так у роботі [7] представлено метод автентифікації, який базується на рекурентних V_k та U_k –послідовностях, а у роботі [8] – метод, який базується виключно на V_k –послідовностях. Представлений в [7] метод, порівняно з відомими аналогами, дозволяє суттєво спростити обчислення, а метод, представлений у [8], забезпечує підвищення криптографічної стійкості процесу автентифікації порівняно з методом, представленим у [7]. Однак запропоновані методи [7, 8] мають певні обмеження щодо часу життя ключа, хоча і в такому представленні мають доволі широке застосування.

Для вирішення вказаної проблеми в роботах [9, 10] запропоновано метод автентифікації сторін взаємодії на основі математичного апарату V_k –послідовностей, який, порівняно з методами, представленими в [7, 8], забезпечує підвищення стійкості за рахунок введення в схему автентифікації додаткового сеансового ключа з боку претендента. Проведено дослідження криптографічної стійкості цього методу на математичному рівні, в результаті якого встановлено, що запропонований метод є більш стійким, ніж відомі аналоги, при цьому метод має ще й значно простішу процедуру завдання параметрів.

Однак актуальним залишається визначення рівня практичної стійкості запропонованого в [9, 10] методу автентифікації сторін взаємодії шляхом дослідження його статистичної безпеки та порівняння його з відомими аналогами – методами Фіата-Шаміра, Фейге-Фіата-Шаміра та Шнорра.

II Дослідження статистичної безпеки методу автентифікації сторін взаємодії на основі V_k –послідовностей

Для дослідження статистичної безпеки методів автентифікації сторін взаємодії використаємо пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite) [11], який на сьогодні є одним з кращих пакетів статистичного тестування криптографічних схем та протоколів. Пакет NIST STS включає в себе набір з 16 статистичних тестів.

Дослідження методів автентифікації сторін взаємодії за допомогою цього пакету тестів будемо здійснювати за такою методикою [12]. Нехай задана двійкова послідовність S довжиною n бітів, тобто $S = \{S_1, S_2, ..., S_n\}$, $S_i \in \{0,1\}$. Для фіксованого значення n формуємо множину з m двійкових послідовностей. Сформована вибірка при цьому складатиме $N = m \times n$.

Далі будемо тестувати за допомогою пакету NIST STS кожну послідовність, сформовану методом, в результаті якого отримаємо статистичний портрет сформованого секретного ключа.

Статистичний портрет послідовності являє собою масив розмірністю $m \times q$, де m – кількість послідовностей, що тестуються, q – кількість статистичних тестів, які використовуються для тестування кожної послідовності. Елементи масиву $P_{i,j} \in [0,1]$, де $i = \overline{1,m}$, $j = \overline{1,q}$, являють собою значення ймовірності, що отримана в результаті тестування i-ї послідовності j-м тестом.

За отриманим статистичним портретом визначаємо долю послідовностей, які пройшли кожен статистичний тест. Для цього задають рівень значимості $\alpha \in [0{,}001; 0{,}01]$ і здійснюють підрахунок значень імовірності P, що перевищує заданий рівень α для кожного з q тестів. У результаті формується вектор коефіцієнтів $R = \{r_1, r_2, ..., r_q\}$, елементи якого характеризують у процентному відношенні проходження послідовності S_i усіх статистичних тестів. Після цього здійснюється статистичний аналіз статистичного портрету. Отримані значення ймовірностей P_{ij} повинні задовольняти рівномірному закону розподілу на інтервалі $[0,1]$.

Заключний висновок щодо методу автентифікації сторін взаємодії будемо приймати таким чином. Будемо вважати, що метод автентифікації G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для усіх $j = \overline{1,q}$ знаходяться всередині довірчого інтервалу $[r_{\min}, r_{\max}]$, де

$$r_{\max(\min)} = (1-\alpha) \pm 3\sqrt{\frac{\alpha(1-\alpha)}{m}}, \qquad (1)$$

і дотримується умова $\chi^2 > 0{,}0001$ для усіх $j = \overline{1,q}$, де χ^2 – критерій підкорення результатів рівномірному закону розподілу на інтервалі $[0,1]$.

Тестування методів автентифікації сторін взаємодії будемо проводити для різних довжин ключів, а саме 512, 768, 1024 бітів. Такий розмір ключів дозволяє виконувати тестування лише для 10 тестів пакету NIST STS, що виключає тест на перевірку рангу двійкової матриці, тест на перевірку шаблонів, що перекриваються, універсальний тест Маурера, тест на перевірку лінійної складності, тест на перевірку випадкових відхилень та модифікований тест на перевірку випадкових відхилень, бо необхідна довжина

послідовностей, що проходять тестування, є недостатньою для успішного проходження чи отримання достовірних результатів даних тестів.

Для виконання тестування було обрано такі параметри:

– довжина послідовності, яка тестується: від 128 до 3072 бітів;

– кількість послідовностей, які тестуються, для кожної довжини ключа, $m = 100$;

– кількість тестів $q = 158$;

– рівень значимості $\alpha = 0{,}001$ та $\alpha = 0{,}01$ відповідно у першому та другому експериментах.

Таким чином маємо: об'єм вибірки від 128 до 3082 бітів для тестування кожного методу автентифікації. Статистичний портрет коду для кожної довжини ключа буде вміщувати в собі 15800 значень імовірності P.

Застосовуючи правило довірчого інтервалу для r_j, обчислюємо значення нижньої границі $r_{\min}$ за формулою (1). Для першого випадку, коли $\alpha = 0{,}001$, це складе

$$r_{\min} = 0{,}999 \pm 3\sqrt{\frac{0{,}999(1-0{,}999)}{100}} = 0{,}98952 ,$$

а для другого випадку, коли $\alpha = 0{,}01$, це складе

$$r_{\min} = 0{,}99 \pm 3\sqrt{\frac{0{,}99(1-0{,}99)}{100}} = 0{,}96015 .$$

Вибір додаткових параметрів зроблено згідно з рекомендаціями, описаними в NIST STS [11].

На основі цих початкових даних проаналізуємо отримані результати тестування послідовностей. У таблицях 1 і 2 наводяться дані про проходження результуючих послідовностей з розміром ключів 512, 768, 1024 бітів відповідно усіма тестами згідно з описаною методикою.

Таблиця 1. Результати тестування методів автентифікації для $\alpha = 0{,}01$ та різних довжин ключів

Метод	**Кількість тестів, які успішно пройшли тестування більше 99% послідовностей**			**Кількість тестів, які успішно пройшли тестування більше 96% послідовностей**		
	512 бітів	***768 бітів***	***1024 бітів***	***512 бітів***	***768 бітів***	***1024 бітів***
V_k	7 (4,43%)	6 (3,80%)	3 (1,90%)	88 (55,70%)	73 (46,20%)	49 (31,01%)
Фейге-Фіата-Шаміра	22 (13,92%)	23 (14,56%)	25 (15,82%)	126 (79,75%)	137 (86,71%)	131 (82,91%)
Фіата-Шаміра	44 (27,85%)	37 (23,42%)	40 (25,32%)	151 (95,57%)	152 (96,20%)	151 (95,57%)
Шнорра	4 (2,53%)	1 (0,63%)	9 (5,70%)	19 (12,03%)	32 (20,25%)	74 (46,84%)

Таблиця 2. Результати тестування методів автентифікації для $\alpha = 0{,}001$ та різних довжин ключів

Метод	**Кількість тестів, які успішно пройшли тестування більше 99% послідовностей**			**Кількість тестів, які успішно пройшли тестування більше 98% послідовностей**		
	512 бітів	***768 бітів***	***1024 бітів***	***512 бітів***	***768 бітів***	***1024 бітів***
V_k	38 (24,05%)	55 (34,81%)	50 (31,65%)	90 (56,96%)	115 (72,78%)	100 (63,29%)
Фейге-Фіата-Шаміра	87 (55,06%)	98 (62,03%)	107 (67,72%)	139 (87,97%)	141 (89,24%)	152 (96,20%)
Фіата-Шаміра	124 (78,48%)	133 (84,18%)	132 (83,54%)	152 (96,20%)	152 (96,20%)	157 (99,37%)
Шнорра	15 (9,49%)	18 (11,39%)	33 (20,89%)	31 (19,62%)	42 (26,58%)	66 (41,77%)

З таблиць 1 та 2 видно, що відсотки проходження тестів за методами Фейге-Фіата-Шаміра та Фіата-Шаміра в рази кращі за метод на основі V_k –послідовностей, проте останній у 3 рази випереджає метод Шнорра при найжорсткіших умовах відбору. При слабкіших умовах спостерігається схожа картина результатів: методи Фейге-Фіата-Шаміра та Фіата-Шаміра у 2 рази випереджають метод на основі V_k –послідовностей, який у свою чергу у 2–3 рази випереджає метод Шнорра. Винятком є довжина ключа 1024 біти, коли в найжорсткіших умовах ($\alpha = 0{,}01$, та рівень проходження 99%) метод Шнорра випередив метод на основі V_k –послідовностей.

Порівняємо результати з рівнем значимості $\alpha = 0{,}001$ за приведеною методикою. В таблиці 3 наведено результати порівняння для різних довжин ключів.

Таблиця 3. Відсотки проходження кожного з 10 тестів для $\alpha = 0{,}001$ та різних довжин ключів

№тесту	Назва статистичного тесту	512 бітів				768 бітів				1024 бітів			
		V_k	Ф-Ф-Ш	Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ф-Ш	Ш
1	Частотний (монобітний) тест	100%	100%	98%	100%	100%	98%	97%	99%	100%	100%	100%	100%
2	Частотний тест всередині блоку	100%	100%	99%	100%	100%	98%	98%	99%	100%	100%	100%	99%
3	Послідовний тест	100%	100%	99%	100%	100%	99%	100%	98%	100%	100%	99%	100%
4	Перевірка максимальної довжини серії в блоці	100%	100%	100%	100%	95%	97%	98%	100%	99%	100%	100%	100%
5	Спектральний тест на основі дискретного перетворення Фур'є	100%	99%	100%	100%	98%	98%	99%	98%	100%	100%	100%	100%
6	Перевірка шаблонів, які не перекриваються	98%	99%	100%	96%	96%	98%	99%	94%	99%	100%	100%	98%
7	Перевірка серій	100%	100%	100%	100%	99%	99%	99%	97%	100%	100%	100%	100%
8	Ентропійний тест	100%	100%	99%	100%	99%	100%	97%	99%	100%	100%	100%	100%
9	Перевірка накоплених сум	100%	100%	98%	100%	100%	98%	97%	99%	100%	100%	100%	100%
10	Перевірка стиснення за алгоритмом Лемпеля-Зіва	100%	100%	98%	100%	100%	98%	97%	99%	100%	100%	100%	100%

Як видно з результатів, наведених у таблиці 3, усі послідовності мають майже однакові показники за всіма видами тестів. При розмірі ключа у 1024 біти найвищі показники має саме метод Фейге-Фіата-Шаміра (усі 100%). Проте, при довжині ключа у 512 біт метод на основі V_k –послідовностей має рівний результат з цим методом (99–100%), що показує його високу стійкість. При довжині ключа у 768 біт, найвищі результати отримав метод на основі V_k –послідовностей.

Порівняємо коди, збільшивши рівень значимості $\alpha = 0{,}01$, що є більш жорстким підходом до оцінки за приведеною методикою. В таблиці 4 наведено результати порівняння для різних довжин ключів.

Таблиця 4. Відсотки проходження кожного з 10 тестів для $\alpha = 0{,}01$ та різних довжин ключів

№тесту	Назва статистичного тесту	512 бітів				768 бітів				1024 бітів			
		V_k	Ф-Ф-Ш	Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ф-Ш	Ш	V_k	Ф-Ф-Ш	Ф-Ш	Ш
1	Частотний (монобітний) тест	99%	100%	95%	100%	100%	98%	97%	99%	99%	99%	98%	100%
2	Частотний тест всередині блоку	98%	99%	97%	100%	100%	98%	98%	99%	99%	98%	100%	98%
3	Послідовний тест	100%	100%	99%	100%	100%	99%	100%	98%	98%	100%	99%	100%
4	Перевірка максимальної довжини серії в блоці	100%	99%	99%	98%	95%	97%	98%	100%	98%	99%	99%	99%
5	Спектральний тест на основі дискретного перетворення Фур'є	100%	97%	99%	98%	98%	98%	99%	98%	99%	100%	98%	99%
6	Перевірка шаблонів, які не перекриваються	97%	98%	99%	93%	96%	98%	99%	94%	95%	98%	99%	96%
7	Перевірка серій	99%	100%	99%	99%	99%	99%	99%	97%	99%	98%	99%	99%
8	Ентропійний тест	99%	100%	98%	99%	99%	100%	97%	99%	99%	100%	98%	100%
9	Перевірка накоплених сум	97%	100%	97%	99%	100%	98%	97%	99%	100%	99%	99%	100%
10	Перевірка стиснення за алгоритмом Лемпеля-Зіва	99%	100%	95%	100%	100%	98%	97%	99%	99%	99%	98%	100%

Як видно з результатів, наведених у таблиці 4, при довжині ключа 512 бітів, високі показники має метод на основі V_k –послідовностей (96–100%). Показовим є спектральний тест на основі дискретного перетворення Фур'є, в якому метод на основі V_k –послідовностей отримав 100%, у той час як усі інші лише 97–99%. При збільшені довжини ключа спостерігається незначне зменшення показників, проте усе одно метод на основі V_k –послідовностей, не на багато, але випереджає існуючі аналоги. Так за частотним, частотним в середині блоку тестах та за тестом перевірки накопичених сум метод на основі V_k –послідовностей показав вищі результати (99–100%), ніж методи Фейге-Фіата-Шаміра, Фіата-Шаміра та Шнорра (97–99%). При найбільшій довжині ключа показники зрівнялись і в усіх методах показують стабільний відсоток проходження тестів на рівні 96–100%.

На рисунках 1–4 представлено статистичні портрети методів автентифікації сторін взаємодії для довжини ключа 512 бітів з вказанням їх параметрів і способів формування.

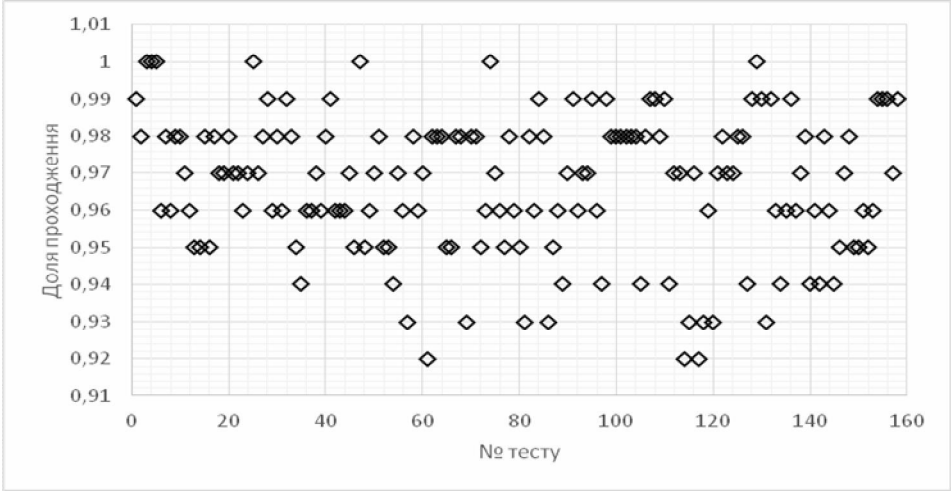

Рисунок 1 – Результати тестування методу автентифікації на основі V_k –послідовностей з розміром ключа 512 бітів

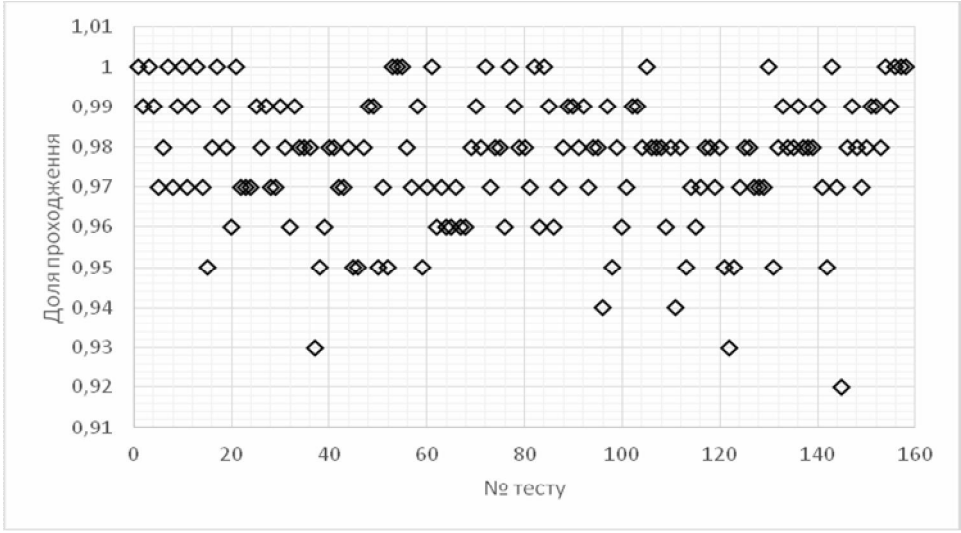

Рисунок 2 – Результати тестування методу автентифікації Фейге-Фіата-Шаміра з розміром ключа 512 бітів

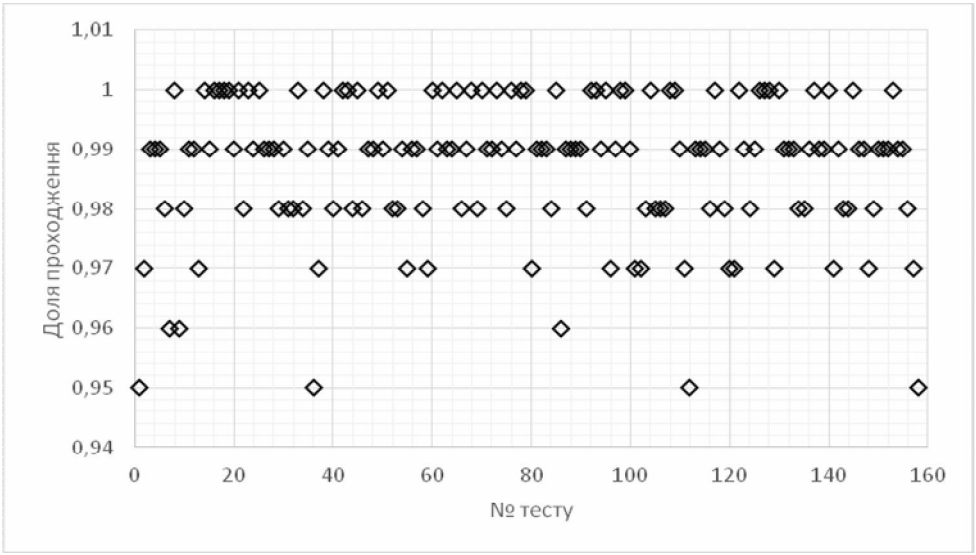

Рисунок 3 – Результати тестування методу автентифікації Фіата-Шаміра з розміром ключа 512 бітів

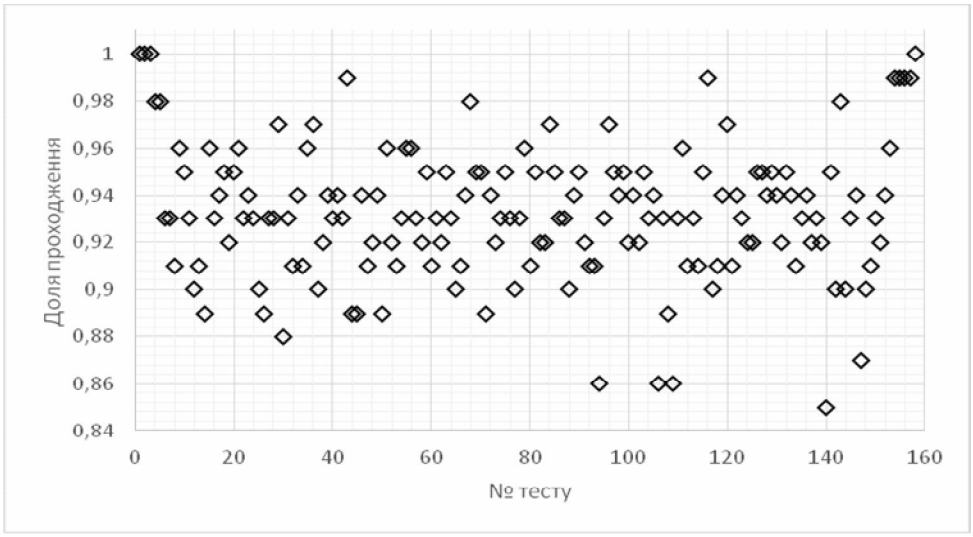

Рисунок 4 – Результати тестування методу автентифікації Шнорра з розміром ключа 512 бітів

Також отримано статистичні портрети результатів тестування методів автентифікації для довжин ключа 768 та 1024 бітів.

Як видно з результатів тестування (рис. 1 – 4), статистичні портрети тримаються у діапазоні від 0,9 до 1. Виключенням є метод Шнорра, у якого нижній поріг досягає 0,85 при довжині ключа 1024 біти. Найвищий нижній поріг спостерігається в методі Фіата-Шаміра (0,95). Кучність статистичних портретів усіх методів свідчить про стабільні показники статистичної безпеки, що є важливим фактором при аналізі стійкості методів. Особливо варто відмітити метод на основі V_k –послідовностей, який має рівномірний розкид показників проходження, що ускладнює виявив його слабких характеристик.

Узагальнимо результати тестування, показавши частку проходження для кожного тесту зі статистичного пакету NIST. На рисунках 5 – 7 показано узагальнені графіки по кожному тесту для кожного методу автентифікації та довжини ключа.

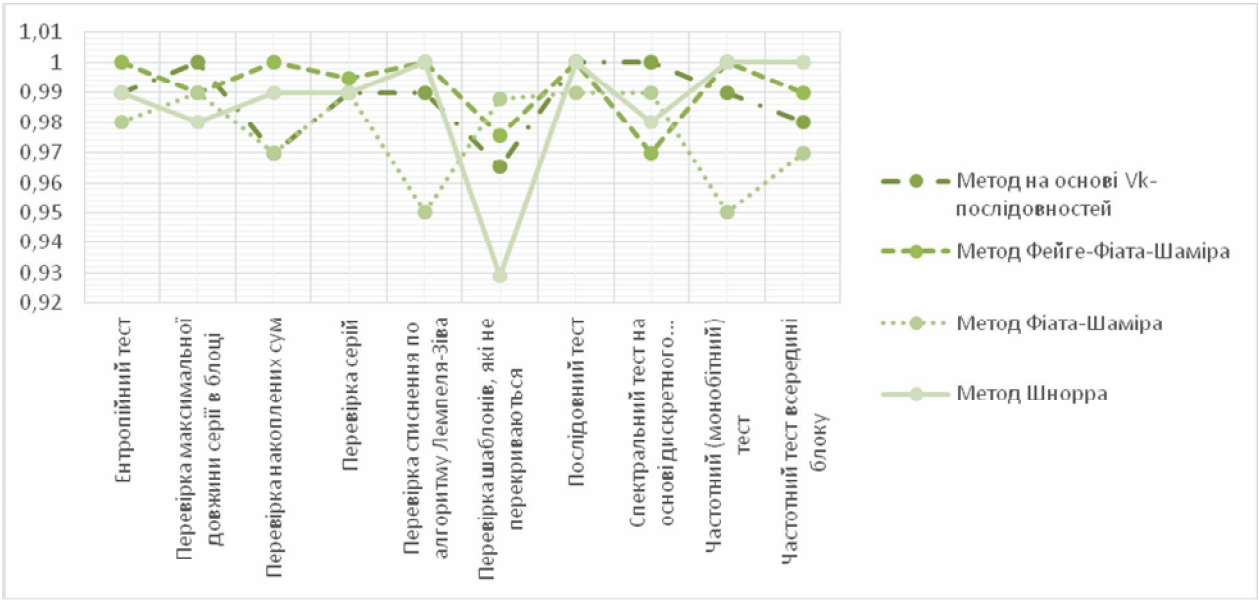

Рисунок 5 – Частка проходження тестів для послідовностей з розміром ключа 512 бітів

Як видно з графіків (рис. 5), майже за усіма тестами найнижчі показники має метод Шнорра, за ним йдуть методи Фіата-Шаміра та Фейге-Фіата-Шаміра. Хоча у частотному тесті всередині блоку метод Шнорра, навпаки, показав найвищий результат. Метод на основі V_k –послідовностей має високі показники, хоча в деяких тестах він програє методам Фіата-Шаміра та Фейге-Фіата-Шаміра, а саме за тестом на перевірку шаблонів, які не перекриваються. Загалом частки проходження за методом на основі V_k –послідовностей знаходяться в межах 0,97-1, в той час як інші мають нижчий нижній поріг (0,93-0,96).

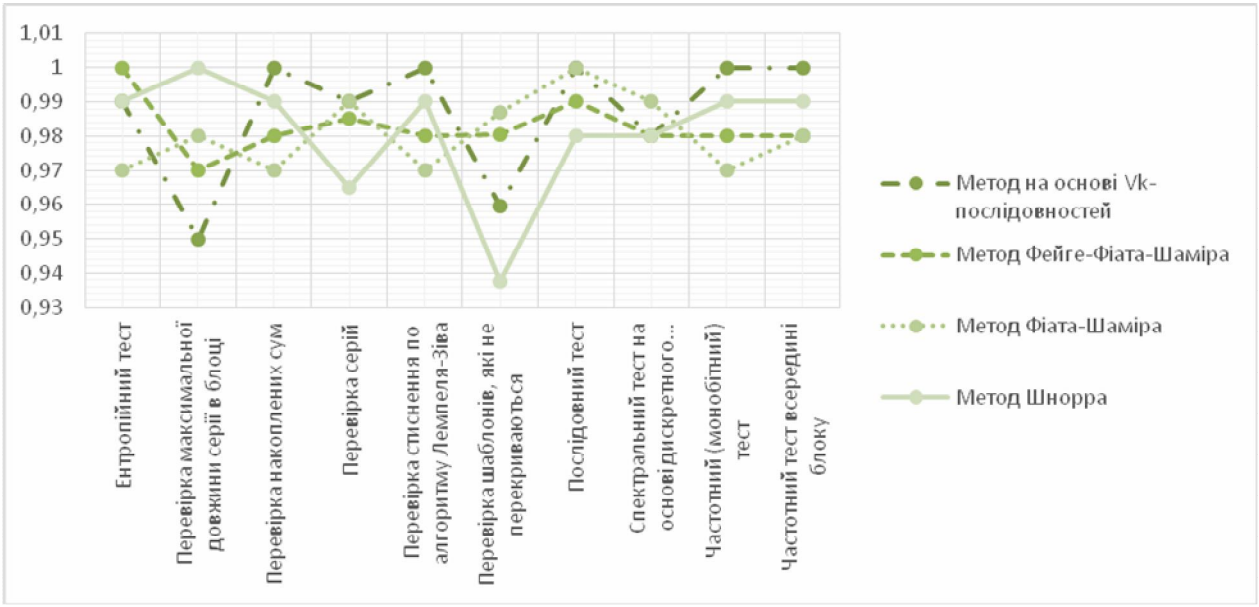

Рисунок 6 – Частка проходження тестів для послідовностей з розміром ключа 768 бітів

Як видно з графіків на рисунку 6, при збільшені довжини ключа частки проходження тестів за методами стають більш різноманітними. У цілому метод на основі V_k –послідовностей має вищі показники, явно поступаючись відомим методам лише за тестом перевірки максимальної довжини серій у блоці. Найнижчі показники усе одно отримує метод Шнорра, а методи Фіата-Шаміра та Фейге-Фіата-Шаміра загалом тримаються середніх позицій.

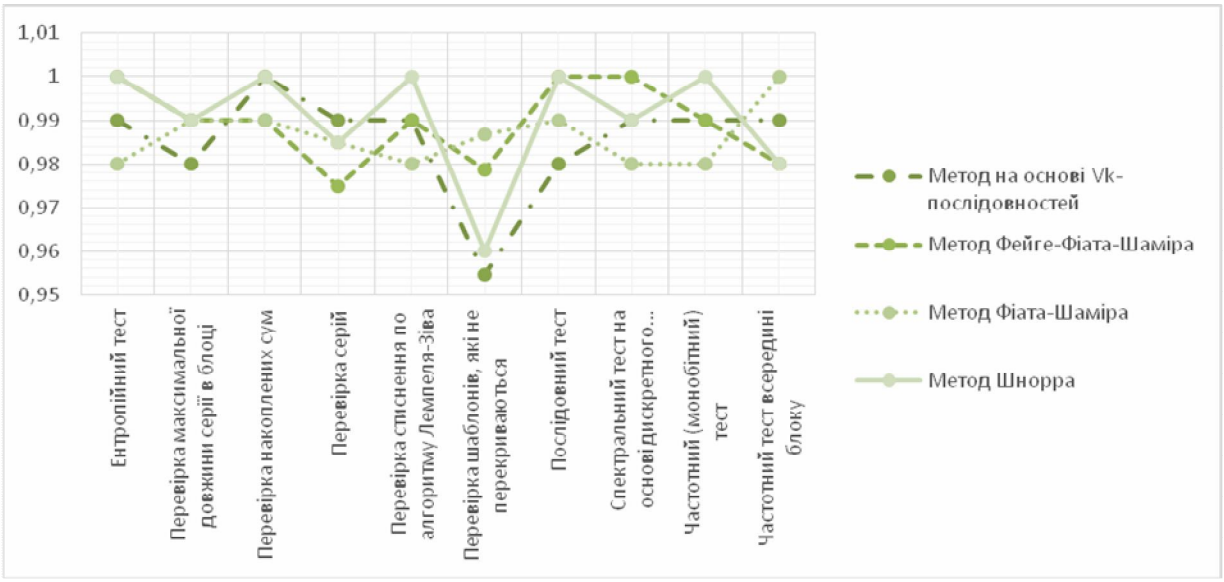

Рисунок 7 – Частка проходження тестів для послідовностей з розміром ключа 1024 бітів

Під час аналізу з найбільшою довжиною ключа у 1024 біти (рис. 7) вимальовується більш однорідна картина, з сильним провалом у тесті на перевірку шаблонів, які не перекриваються (рівень до 0,955 порівняно з 0,98-1). Загалом вищі показники має метод Шнорра, проте в тестах на перевірку серій, перевірку шаблонів та спектральному тесті його випереджають інші методи, а саме метод на основі V_k – послідовностей та метод Фейге-Фіата-Шаміра відповідно. Слід відзначити, що метод на основі V_k – послідовностей показує стабільно високі та середні результати, що характеризує його з гарного боку.

III Висновки

Дослідження запропонованого в [9, 10] методу автентифікації сторін взаємодії на основі V_k – послідовностей з відомими методами автентифікації Фейге-Фіата-Шаміра, Фіата-Шаміра та Шнорра показало, що в цілому запропонований метод автентифікації володіє як мінімум не гіршими, а в деяких випадках кращими, значеннями показників.

Нижчі значення запропонований метод показує за показником проходження тестів результуючими послідовностями при рівні значимості $\alpha = 0{,}01$, при зниженні межі значимості відставання зменшується від існуючих аналогів. Так при довжині ключа у 768 біт, метод на основі V_k –послідовностей в рази (68–72% порівняно з 26%) випереджає метод Шнорра і лише на 10–15% відсотків відстає від методів Фейге-Фіата-Шаміра, Фіата-Шаміра.

Порівняння за окремими тестами показує, що метод на основі V_k –послідовностей має вищі показники (98–100%) порівняно з відомими методами (96–99%). При збільшенні довжини ключа ці показники вирівнюються, що говорить про явно кращі можливості використання запропонованого методу при автентифікації саме з малими довжинами ключів.

Загальна картина тестування показує, що метод на основі V_k –послідовностей тримається на високому рівні, у той час як інші методи мають якщо не низькі (метод Шнорра), то нестабільні показники (методи Фейге-Фіата-Шаміра, Фіата-Шаміра).

За результатами тестування можна зробити загальний висновок, що запропонований метод автентифікації на основі V_k –послідовностей має стабільно високі показники, що є гарною характеристикою його статистичної безпеки. Особливо це помітно при малих довжинах ключів, що, в першу чергу, з кращого боку рекомендує його застосування в системах автентифікації, де використання великих ключів не є важливим, однак забезпечення рівня статистичної безпеки буде вищим.

Список використаної літератури: ***1.*** *Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия–Телеком, 2007. – 320 с.* ***2.*** *Menezes A. J., van*

Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p. ***3.*** *Fiat A., Shamir A. How to Prove Yourself: Practical Solutions to Identification Signature Problems // Proceedings of Advances in Cryptology CRYPTO '86, Springer-Verlag, 1987. – P. 186–194.* ***4.*** *Feige U., Fiat A., Shamir A. Zero Knowledge Proofs of Identity // Proceedings of the lPth Annual ACM Symposium on the Theory of Computing, 1987. – P. 210–217.* ***5.*** *Guillou L.C., Quisquater J.-J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory // Proceedings of Advances in Cryptology EUROCRYPT'88, Springer-Verlag, 1988. – P. 123–128.* ***6.*** *Schnorr C.P. Efficient Signature Generation for Smart Cards // Proceedings of Advances in CRYPTO '89, Springer-Verlag, 1990. – P. 239–252.* ***7.*** *Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – №1, 2013. – С. 4–10.* ***8.*** *Яремчук Ю. Є. Можливість автентифікації сторін взаємодії на основі рекурентних послідовностей // Захист інформації. – Том 15, №4, 2013. – С. 394–398.* ***9.*** *Патент України на корисну модель № 84271, (51) МПК (2013.01) H03M 13/00. Спосіб автентифікації сторін взаємодії на основі електронного коду / Ю. Є. Яремчук. – № заявки u2013 06319; заявл. 22.05.2013; опубл. 10.10.2013, бюл. №19.* ***10.*** *Яремчук Ю. Є. Методи автентифікації на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.* ***11.*** *NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo. – National Institute of Standards and Technology, 2010. – 131 p.* ***12.*** *Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.*

Юрій Васильєв
ДержНДІ Спецзв'язку

УДК 004.056

АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ ЩОДО ВИЗНАЧЕННЯ КЛЮЧОВИХ СИСТЕМ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: ***Наведено міжнародний досвід у нормативному визначені ключових системам інформаційної інфраструктури.***
Summary: ***Regulatory identify systems of key information infrastructure.***
Ключові слова: ***Інформація, інформаційна безпека, ключові системи інформаційної інфраструктури***

I Вступ

У кожному суспільстві можливо виділити сектори, системи або мережі, від яких життєво залежить суспільство і порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівні. Комплекс цих секторів, систем або мереж почали називати ключовими або критичними системами інформаційної інфраструктури (далі - КСІІ).

Багато держав, а також терористичних та кримінальних структур інтенсивно вдосконалюють методи і способи використання інформаційних технологій та засобів для деструктивних інформаційних впливів на інформаційні ресурси інформаційно-телекомунікаційних систем і мереж державних та недержавних організацій. Таке застосування інформаційних технологій та засобів надає їм властивості так званої інформаційної зброї. Для нанесення значного збитку інтересам держави і суспільства інформаційна зброя може бути застосована і в мирний час, особливо терористичними організаціями. При цьому порушення функціонування КСІІ може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, нанесенням великої матеріальної, фінансової, економічної шкоди або великомасштабними порушеннями життєдіяльності міст та населених пунктів і т.п. У цих умовах важливу роль відіграє державне регулювання діяльності щодо забезпечення безпеки інформації в КСІІ.

Необхідно зазначити, що на даний час в Україні проблематика, що пов'язана з визначенням КСІІ, оцінюванням актуальних загроз безпеки, побудовою систем захисту та нормативно-правовим забезпеченням цих процесів знаходяться на початковому рівні та наполегливо потребує розвитку.

У зв'язку з нарощуванням з 1998-го року загрози тероризму в розвинених країнах почалися дискусії про уразливість національних інфраструктур. Аналізи були направлені не тільки на кібернетичні інфраструктурні системи, але і на решту областей і секторів забезпечення життя суспільства. У США PRESIDENTIAL DECISION DIRECTIVE/NSC-63 [1] визначили КСІІ як основні системи, які можуть мати матеріальну або кібернетичну платформу і мають дію на функціональність економіки держави. Ці основні системи вбирали в