УДК 004.056.55:004.312.2

В. М. Рудницький, В. В. Ларін, А. І. Нікорчук

ПРАКТИЧНА РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ ТЕХНОЛОГІЇ СЕТ-ШИФРУВАННЯ

Проведено оцінювання статистичних властивостей результатів СЕТ-шифрування операцій перестановок, керованих інформацією. Досліджено можливість застосування СЕТ-операцій у потоковому шифруванні під час послідовного перетворення елементів відкритої інформації.

Розроблено архітектуру системи захисту інформації з урахуванням криптографічного перетворення у разі застосування СЕТ-операцій, керованих інформацією, та запропоновано функціональні схеми реалізації елементарних функцій відповідно до завдань.

Тестування програмної реалізації розробленого методу захисту інформації проведено за допомогою згенерованих псевдовипадкових послідовностей програмним пакетом тестів NIST STS. Оцінювання результатів дослідження дало змогу дійти висновку, що розроблений метод криптографічного захисту на основі СЕТ-операцій, керованих інформацією, прийнятний для використання у системах озброєння та військової техніки.

Показано, що генератори псевдовипадкових послідовностей є базовими складниками досліджуваної системи захисту, надійність роботи яких переважно керується конкретно можливостями використовуваних генераторів. Стійкі псевдовипадкові послідовності, які за своєю сутністю є обмежені, мають майже всі особливості реалізацій реально випадкових процесів та успішно замінюють їх, оскільки випадкові послідовності надзвичайно складно формувати.

Ключові слова: *оцінювання, СЕТ-операція, генератор псевдовипадкових послідовностей, статистичні властивості, синтез, модель, NIST STS.*

Постановка проблеми. Псевдовипадкова послідовність (ПВП) – це послідовність значень, яка отримана за визначеними арифметичними правилами, але водночас з урахуванням усіх заданих властивостей випадкової послідовності значень у межах конкретної розв’язуваної задачі [18].

Важливою умовою для використання псевдовипадкової послідовності є відповідність певним вимогам. У згенерованих послідовностях необхідними індикаторами випадковості й одноманітності, які перевіряються за допомогою статистичних тестів, є також умови непередбачуваності послідовності.

Наразі є чимало різноманітних стандартів і алгоритмів захисту інформаційного ресурсу, які комплексно застосовуються для захисту інформаційного ресурсу, що циркулює у мережі в режимі реального часу [16, 20]. Під стандартами захисту інформаційного ресурсу розуміється комплекс технічних специфікацій і команд, метою яких є забезпечення конфіденційності, цілісності та доступності інформаційного ресурсу. Зазначені стандарти класифікуються двома способами: стандарти інформаційної безпеки і стандарти управління інформаційною безпекою. Інформаційна безпека охоплює стандарти і структури, що зосереджені на таких засобах безпеки, як ISO/IEC27000 серії та NIST.

Національний інститут стандартів і технологій США (NIST) розробляє стандарти кібербезпеки, рекомендації, правила, найкращі практики та інші інструменти. Для того, щоб надавати точну інформацію для довгострокових досліджень, які передбачають розвиток технологій і майбутні виклики, NIST пропонує більш ніж тисячу стандартних довідкових матеріалів [14–17].

Вибір відповідних стандартів захисту інформаційного ресурсу має значний вплив на захист інформації, яка циркулює в мережі в режимі реального часу [6, 7, 8]. Ці чинники мають достатню кількість складових управління, які можна застосувати як базис для захисту інформації в системах озброєння та військової техніки. Залежно від конкретних завдань, складу, структури та вимог вибирають формат захисту каналу управління і зв’язку.

Найбільш сучасною, точною та гарантованою методикою є тестування статистичних властивостей NIST STS [18], і тому було вибрано саме цей пакет для аналізу проведених досліджень.

Аналіз останніх досліджень і публікацій. Базові основи розроблення і впровадження малоресурсних потокових шифрів розглянуто у [1, 19]. У цих працях наведено прикладні аспекти застосування СЕТ-операцій. Значущість технологій СЕТ-шифрування для визначення й оцінювання шляхів удосконалення відомих і розроблення нових криптографічних протоколів досліджено у публікаціях [2, 3].

Класифікацію СЕТ-операцій за кількістю операндів на одноопераднді, двохоперандні, трьохоперандні і т. ін. подано у [4, 5]. Для побудови криптографічних систем запропоновано використовувати багатоопераднді СЕТ-операції. Технології побудови двохоперандних операцій наведено у джерелах [3, 4, 5].

Автори у [2] пропонують використовувати дискретно-казуальне представлення схем елементарних функцій і СЕТ-операцій, зокрема й СЕТ-операцій, керованих інформацією.

Генератори псевдовипадкової послідовності застосовують у багатьох напрямах, таких, як інформаційні й телекомунікаційні технології [12, 18], захист інформації в комп'ютерних системах і мережах [13, 14, 15], математичне моделювання, оброблення інформаційного ресурсу, генерація псевдовипадкових послідовностей тощо. У переважній більшості криптографічних алгоритмів випадкові числа використовуються як вхідний масив у певних точках [16] або як ключ у системах потокового шифрування [17].

Основні результати дослідження операцій малоресурсних криптографічних систем і результати криптоперетворень наведено у публікаціях [1–5, 19].

Метою статті є проведення оцінювання статистичних властивостей результатів СЕТ-шифрування операцій перестановок, керованих інформацією.

Виклад основного матеріалу. Для дослідження криптографічних алгоритмів й оцінювання якості генераторів ПВП використовуються різноманітні програмні комплекси, серед яких на особливу увагу заслуговують: система оцінювання статистичних властивостей DIEHARD, пакет NIST STS (США) [18], система оцінювання статистичної безпеки алгоритмів генерації ПВП і криптоалгоритмів.

Система оцінювання статистичних властивостей DIEHARD має низку недоліків, а саме: параметри тестування жорстко фіксовані; бракує довідкової служби й методики трактування результатів оброблення; деякі тести не мають змістовного обґрунтування [18].

Інженерами NIST [Національний інститут стандартів і технологій (НІСТ) США] у межах проєкту AES (Advanced Encryption Standard) було розроблено набір статистичних тестів «NIST STS» (NIST Statistical Test Suite) і запропоновано методику проведення статистичного тестування генераторів псевдовипадкових чисел, орієнтованих на використання у завданнях криптографічного захисту інформації, яка, на думку фахівців у цій сфері, нині найкраще відповідає вимогам усіх зацікавлених сторін [16, 17, 18].

Простота дискретно-казуального представлення моделей елементарних функцій перестановок, керованих інформацією, забезпечила простоту представлення моделей одноопераднді СЕТ-операцій перестановок, керованих інформацією. Уперше наведена базова група одноопераднді СЕТ-операцій перестановок, керованих інформацією, містить лише симетричні операції, кожна з яких реалізує пряме й обернене перетворення.

Основною гіпотезою дослідження є наявність можливості об'єднання одноопераднді СЕТ-операцій перестановок, керованих інформацією, у двохоперандні операції на основі застосування дискретно-казуальних моделей.

Доведення висунутої гіпотези передбачає використання дискретно-казуальних моделей елементарних функцій перестановок, керованих інформацією, для побудови моделей одноопераднді і двохоперандних СЕТ-операцій. Для встановлення взаємозв'язків між моделями одноопераднді СЕТ-операцій у кортежі двохоперандної СЕТ-операції та її модифікації використовували методи дискретної математики, теорії множин та ситуаційного управління.

Проєктування легких шифрів передбачає зменшення складності алгоритмів перетворення інформації у разі бажаного збереження їх криптостійкості. Серед трирозрядних елементарних функцій, на основі яких будуються СЕТ-операції, одними з найпростіших за апаратною реалізацією вважаються елементарні функції перестановок, керованих інформацією [2]. Їхня функціональна складність аналогічна складності пристрою порозрядного додавання за модулем 2 (рисунок 1).

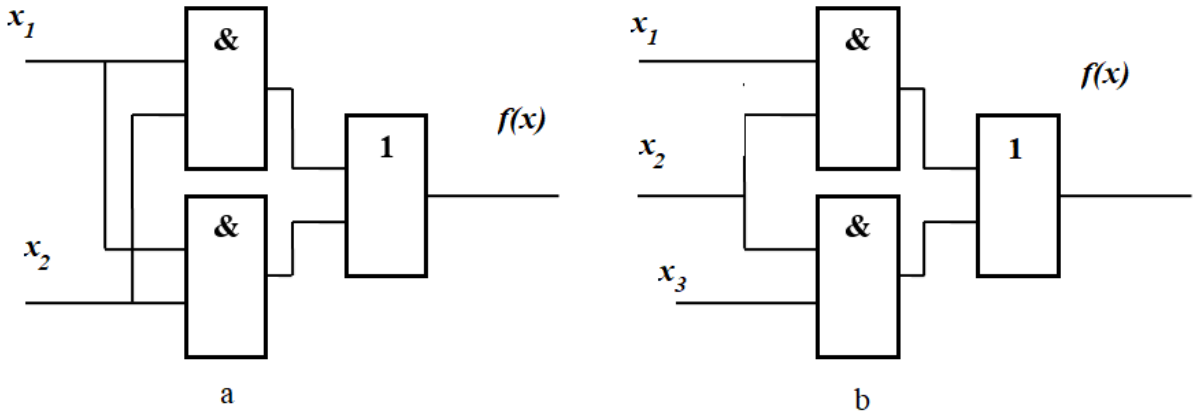

Рисунок 1 – Функціональні схеми реалізації елементарних функцій додавання за модулем 2 (*а*) і перестановки, керованої інформацією (*б*) *(розроблено авторами)*

Незначна складність реалізації елементарних функцій перестановки, керованої інформацією, забезпечує доцільність їх застосування у малоресурсних системах потокового шифрування. Дослідимо ймовірність отримання дискретно-казуальних моделей елементарних функцій, одно- і двохоперендних СЕТ-операцій перестановок, керованих інформацією.

Дискретно-казуальна модель являє собою казуальне поєднання трьох дискретних функцій [2]:

$$f(x) = (f_1(x))\big(f_2(x)\big)\big(f_3(x)\big), \quad (1)$$

де$f_2(x)$ – функція керування;

$f_1(x)$ і $f_3(x)$ – перша і друга функції перетворення; за умови $f_2(x)$буде виконуватися перша функція перетворення $(f_1(x))$, в іншому разі – друга функція перетворення $\big(f_3(x)\big)$.

Елементарну функцію перестановки, керованої інформацією, що зображена на рисунку 1, відповідно до (1) можна описати моделлю:

$$f(x) = (x_1)(x_2)(x_3). \quad (2)$$

Для вдосконалення методів синтезу елементарних функцій і СЕТ-операцій перестановок, керованих інформацією, необхідні такі властивості дискретно-казуальної моделі (1):

– інверсія результату реалізації функції керування приведе до перестановки місцями функцій перетворення:

$$f(x) = (f_1(x))\big(f_2(x)\big)\big(f_3(x)\big) = (f_3(x))\big(f_2(x)\big)\big(f_1(x)\big);$$

– інверсія результатів реалізації функцій перетворення приведе до інверсії реалізації такої моделі:

$$\overline{(f_1(x))}\big(f_2(x)\big)\overline{\big(f_3(x)\big)} = f(x)$$

З використанням моделі (2) можна побудувати всі елементарні функції перестановок, керованих інформацією.

1. На основі перестановок трьох дискретних функцій $f_1(x) = x_1$, $f_2(x) = x_2$ і $f_3(x) = x_3$ побудувати шість дискретно-казуальних моделей: $f(x) = (x_1)(x_2)(x_3)$; $f(x) = (x_1)(x_3)(x_2)$; $f(x) = (x_2)(x_1)(x_3)$; … ;.

2. Із кожної побудованої моделі шляхом інверсії функцій перетворення

побудувати по чотири дискретно-казуальні моделі: $f(x) = (x_1)(x_2)(x_3)$;

$f(x) = (x_1)(x_2)(x_3)$; $f(x) = (x_1)(x_2)(x_3)$; $f(x) = (x_1)(x_2)(x_3)\ldots$

3. На основі другої властивості поділити отримані дискретно-казуальні моделі на прямі та інверсні.

Результати синтезу моделей елементарних функцій перестановок, керованих інформацією, наведені у таблиці 1.

Таблиця 1 – Множина синтезованих моделей елементарних функцій перестановок, керованих інформацією *(розроблено авторами)*

Елементарні функції перестановок, керованих інформацією			
прямі		інверсні	
1	$f(x) = (x_1)(x_2)(x_3)$	13	$f(x) = (\overline{x_1})(x_2)(\overline{x_3})$
2	$f(x) = (x_1)(x_2)(\overline{x_3})$	14	$f(x) = (\overline{x_1})(x_2)(x_3)$
3	$f(x) = (x_1)(x_3)(x_2)$	15	$f(x) = (\overline{x_1})(x_3)(\overline{x_2})$
4	$f(x) = (x_1)(x_3)(\overline{x_2})$	16	$f(x) = (\overline{x_1})(x_3)(x_2)$
5	$f(x) = (x_2)(x_1)(x_3)$	17	$f(x) = (\overline{x_2})(x_1)(\overline{x_3})$
6	$f(x) = (x_2)(x_1)(\overline{x_3})$	18	$f(x) = (\overline{x_2})(x_1)(x_3)$
7	$f(x) = (x_2)(x_3)(x_1)$	19	$f(x) = (\overline{x_2})(x_3)(\overline{x_1})$
8	$f(x) = (x_2)(x_3)(\overline{x_1})$	20	$f(x) = (\overline{x_2})(x_3)(x_1)$
9	$f(x) = (x_3)(x_1)(x_2)$	21	$f(x) = (\overline{x_3})(x_1)(x_2)$
10	$f(x) = (x_3)(x_1)(\overline{x_2})$	22	$f(x) = (\overline{x_3})(x_1)(x_2)$
11	$f(x) = (x_3)(x_2)(x_1)$	23	$f(x) = (x_3)(x_2)(x_1)$
12	$f(x) = (x_3)(x_2)(x_1)$	24	$f(x) = (x_3)(x_2)(x_1)$

Побудована група дискретно-казуальних моделей елементарних функцій перестановок, керованих інформацією, дає змогу перейти до моделювання одноопераднихCET-операцій перестановок, керованих інформацією.

Проведемо оцінку ймовірності правильного виявлення статистичних властивостей результатів заданого криптографічного перетворення невипадкової монотонно зростаючої послідовності із циклом повторення 256 байтів, в яку записані коди чисел 0, 1, 2, …, 255.

Порядок формування послідовності на основі CET-операцій перестановок, керованих інформацією, подано на рисунку 2. Він показує повний цикл оброблення CET-операцій, керованих інформацією.

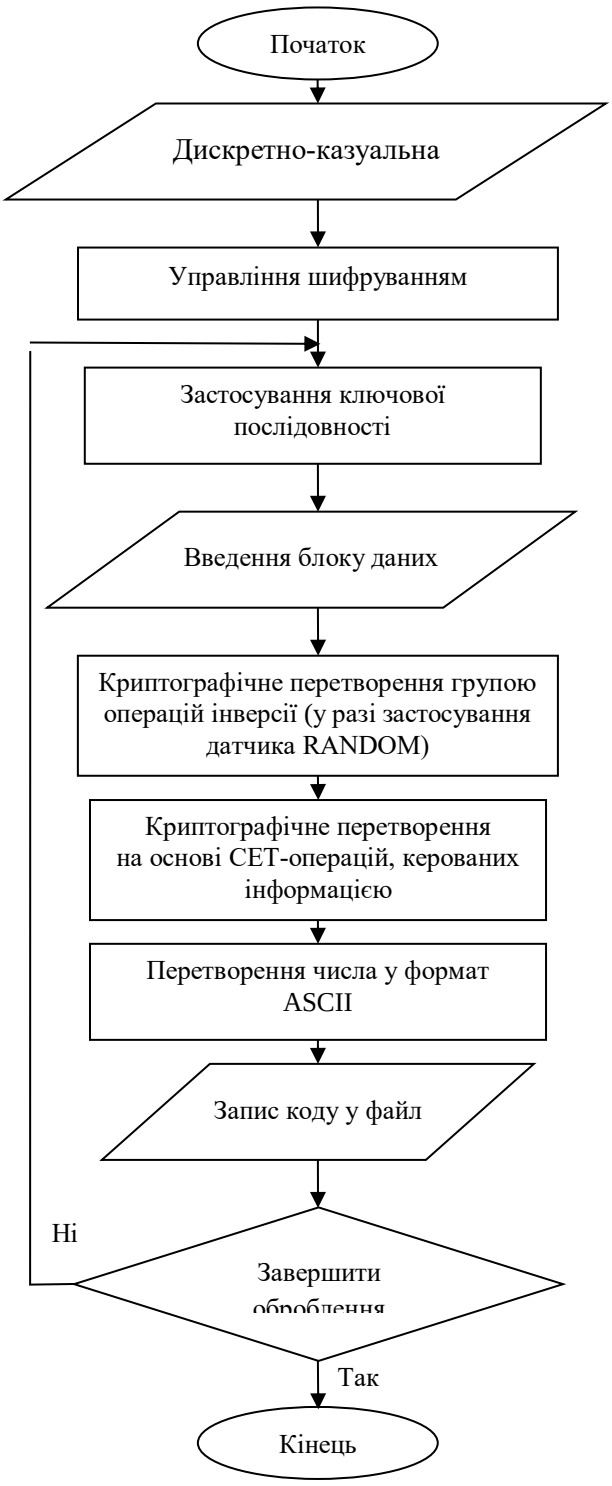

Рисунок 2 – Алгоритм формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією *(розроблено авторами)*

Проведено тестування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, з використанням програмного пакету NIST STS.

Зведені результати тестування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, із циклом повторення 256 байтів програмним пакетом NIST STS подано у таблиці 2.

Таблиця 2 – Зведені результати тестування *(розроблено авторами)*

Генератор	Кількість тестів, у яких тестування пройшло	
	99 % послідовних	96 % послідовних
Криптографічне перетворення на основі СЕТ-операцій, керованих інформацією	136 (71,9 %)	188 (99,5 %)

Результати тестування показали, що метод захисту інформації на основі СЕТ-операцій перестановок, керованих інформацією, у межах контрольного діапазону за методикою NIST STS.

Перевіримо статистичні властивості результатів криптографічного перетворення на основі СЕТ-операцій, керованих інформацією, на прикладі досліджуваного інформаційного ресурсу.

Статистичний портрет програмної реалізації алгоритму формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, із циклом повторення 256 байтів подано на рисунку 3.

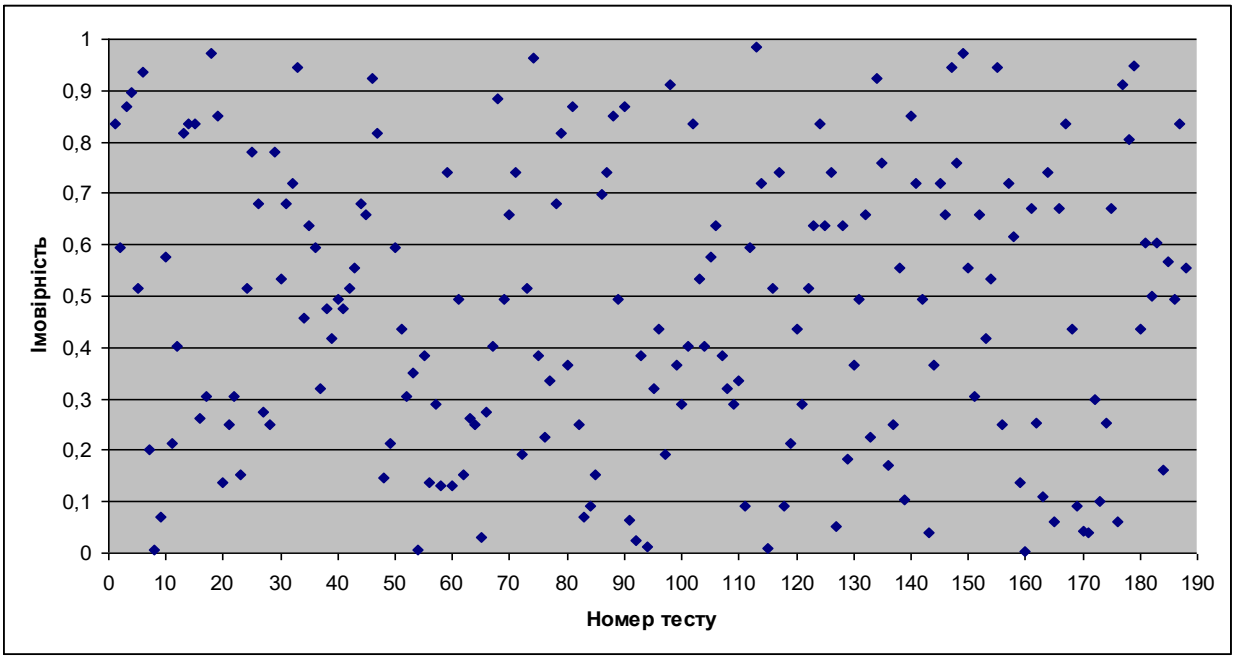

Рисунок 3 – Статистичний портрет програмної реалізації алгоритму формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією *(розроблено авторами)*

З урахуванням програмної реалізації розробленого методу захисту інформації проведено дослідження згенерованих псевдовипадкових послідовностей програмним пакетом тестів NIST STS. Оцінювання результатів тестування дало змогу дійти висновку, що запропонований метод формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, є прийнятним для використання у системах захисту інформаційних ресурсів системи озброєння та військової техніки.

Як видно з отриманих результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [18].

Висновки

У статті на основі узагальнення отриманих результатів проведено оцінювання статистичних властивостей результатів шифрування із застосуванням СЕТ-операцій перестановок, керованих інформацією.

Підвищити швидкість роботи системи управління і зв’язку у разі застосування СЕТ-операцій перестановок, керованих інформацією, можна шляхом управління процесом шифрування. Один із

варіантів реалізації алгоритму формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, зображено на рисунку 2.

Практична реалізація алгоритму формування послідовності на основі СЕТ-операцій перестановок, керованих інформацією, залежить від вимог до розроблення систем криптографічного захисту інформаційного ресурсу.

Реалізація СЕТ-операцій перестановок, керованих інформацією, на основі псевдовипадкової (гамуючої) послідовності відповідає вимогам програмного пакету статистичного тестування NIST STS.

Напрямом подальшого дослідження є побудова груп некомутативних двохоперандних СЕТ-операцій перестановок, керованих інформацією, для застосування у перспективних сценаріях малоресурсного потокового шифрування.

Перелік джерел посилання

1. Rudnytskyi V., Lada N., Kuchuk G. & Pidlasyi D. Architecture of CET-operations and stream encryption technologies : monograph. Cherkasy : R. V. Ponomarenko 2024. 374 p. URL: https://surl.li/hfzghl (accessed: 14.10.2024).

2. Rudnytskyi V., Lada N., Pochebut M., Melnyk O. & Tarasenko Ya. Increasing the cryptographic strength of CETencryption by ensuring the transformation quality of the information block. 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Oct. 13–15, 2023, Athens, Greece. P. 1–6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416546.

3. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19. № 1. С. 56–59. URL: https://surli.cc/duunzv (дата звернення: 14.10.2024).

4. Рудницький В. М., Ларін В. В., Мельник О. Г., Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. *Системи управління, навігації та зв'язку*. 2023. № 4. С. 96–101. DOI: https://doi.org/10.28925/2663-4023.2024.23.616.

5. Рудницька Ю. В., Рудницький С. В. Моделювання симетричних операцій криптографічного кодування. *Проблеми інформатизації* : тези доп. 10-ї міжнар. наук.-техн. конф., Черкаси – Баку – Бельсько-Бяла – Харків, 24-25 листоп. 2022 р. Черкаси : ЧДТУ; Баку : ВА ЗС АР, Бельсько-Бяла : УТіГН, Харків : НТУ «ХПІ», 2022. Т. 2. С. 10.

6. Dhaou I. B., Skhiri H., Tenhunen H. Study and Implementation of a Secure Random Number Generator for DSRC Devices. In Proceedings of the 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), Manama, Bahrain, 8–11 May 2017. P. 1–9.

7. Nguyen-Duc A., Viet Do M., Quan L., Nguyen Khac K., Nguyen Quang A. On the adoption of static analysis for software security assessment. A case study of an open-source e-government project. Comput. Secur. 2021.

8. Choi J. Physical Layer Security for Channel-Aware Random Access with Opportunistic Jamming. IEEE Trans. Inf. Forensics Secur. 2017, 12. P. 2699 – 2711.

9. Tang J., Jiao L., Zeng K., Wen H., Qin K. Y. Physical Layer Secure MIMO Communications Against Eavesdroppers with Arbitrary Number of Antennas. IEEE Trans. Inf. Forensics Secur. 2021, 16. P. 466–481.

10. Gergely A. M., Crainicu B. A succinct survey on (Pseudo)-random number generators from a cryptographic perspective. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017. Vol. 42. P. 1–6.

11. Wang P., You F., He S. Design of Broadband Compressed Sampling Receiver Based on Concurrent Alternate Random Sequences. IEEE Access 2019, 7. P. 525–538.

12. Benedetti R., Andreano M. S., Piersimoni F. Sample selection when a multivariate set of size measures is available. Stat. Methods Appl. 2019, 28. P. 1–25.

13. Tuncer T., Avaroglu E. Random number generation with LFSR based stream cipher algorithms. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017. Vol. 42. P. 171–175.

14. Chithaluru P., Tanwar R. and Kumar S. Cyber-attacks and their impact on real life. *Information security and optimization*. 2020, Chapman and Hall/CRC. P. 61–77.

15. Khan A., Bryans J. and Sabaliauskaite G. Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434. Applied Cryptography and Network

Security Workshops: ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Rome, Italy, June 20–23, 2022, Proceedings. 2022. Springer.

16. Taherdoost H. Understanding Cybersecurity Frameworks and Information Security Standards. A Review and Comprehensive Overview. *Electronics*, 2022. 11 (14). P. 2181.

17. Hijji M. and Alam G. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, 2022. 22. P. 86.

18. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto, J. Nechvatal et al. URL : https://surl.lu/jsuhvq (accessed: 14.10.2024).

19. Hatzivasilis G., Fysarakis K., Papaefstathiou I., Manifavas Ch. A review of lightweight block ciphers. *Cryptographic Engineering.* 2018. Vol. 8 (2). P. 141–184. DOI: https://doi.org/10.1007/s13389-017-0160-y.

20. Шугуров О. С. Розвиток військових наземних роботизованих систем в контексті нових концепцій управління: перспективи України. *Стратегічні пріоритети.* 2007. № 4. С. 198–205. URL: https://surl.li/pifinl (дата звернення: 14.10.2024).

Стаття надійшла до редакції 15.02.2025 р.

UDC 004.056.55:004.312.2

V. Rudnytskyi, V. Larin, A. Nikorchuk

PRACTICAL IMPLEMENTATION OF INFORMATION PROTECTION RESULTS BASED ON CET ENCRYPTION TECHNOLOGY

The article evaluates the statistical properties of the results of CET-encryption of information-driven permutation operations. The possibility of using CET-operations in stream encryption in sequential transformation of open information elements is investigated.

Based on the generalization of the obtained results, a method of cryptographic transformation based on information-driven CET-operations is developed.

The structure of an information protection system based on cryptographic transformation based on information-driven CET-operations is proposed and functional models of devices for their hardware implementation are developed.

Based on the implemented software implementation of the information protection method, the generated pseudorandom sequences are tested using the NIST STS test software package. Analysis of the test results made it possible to conclude that the proposed method of cryptographic transformation based on information-driven CET-operations is suitable for use in information resource protection systems.

Pseudorandom sequence generators are the most important elements of any protection system, the reliability of which is largely determined by the properties of the generators used. Qualitative pseudorandom sequences, which are inherently deterministic, have almost all the properties of implementations of truly random processes and successfully replace them, since random sequences are extremely difficult to form.

Discrete-casual models of elementary functions of information-driven permutations were constructed. The properties of these models were established, which allowed to simplify the method of their synthesis.

Only two-operand CET-operations of the basic group of operations, which were obtained according to the results of the experiment, were used. This limitation is due to the possibility of constructing a complete group of models of one-operand CET-operations of information-driven permutations from models of one-operand CET-operations of the basic group.

***Keywords**: evaluation, CET-operation, pseudorandom sequence generator, statistical properties, synthesis, model, NIST STS.*

Рудницький Володимир Миколайович – доктор технічних наук, професор, головний науковий співробітник, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

https://orcid.org/0000-0003-3473-7433

Ларін Володимир Валерійович – кандидат технічних наук, доцент, докторант штатний, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

https://orcid.org/0000-0003-0771-2660

Нікорчук Андрій Іванович – кандидат технічних наук, доцент, докторант, Національна академія Національної гвардії України

https://orcid.org/ 0000-0003-2683-9106