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 research paper provides the evaluation of statistical properties of the results for CET encryption of information-driven permutation operations. The study also investigates a possibility of applying CET operations in stream encryption during the sequential transformation of elements of open information.

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

Considering the software implementation of the information security method, the generated pseudorandom sequences were tested with the NIST STS. The analysis of the test results has led to the conclusion that the proposed method of cryptographic transformation based on information-driven CET operations is suitable for use in weapons and military equipment systems.

It is shown that pseudorandom sequence generators are the most important elements of any security system, and their reliability is largely determined by the properties of the used generators. High-quality pseudorandom sequences, which are inherently deterministic, have virtually all the properties of implementations of truly random processes and successfully replace them, since random sequences are extremely difficult to generate.

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

Statement of the problem. The pseudorandom sequence (PRS) is defined as a sequence of numbers produced according to some specific rules of arithmetic, but it has all the properties of a random sequence of numbers within a particular problem being solved [18].

An important condition for using a pseudo-random sequence is that it meets certain requirements. In the generated sequences, conditions for unpredictability of the sequence serve as the indicators required for randomness and uniformity that are checked using statistical tests.

There is an array of standards and protocols for protecting an information resource that can be adopted systematically to protect data circulating in the network in real time [16, 20]. Cybersecurity standards are technical specifications and guidelines aimed at ensuring the confidentiality, integrity and availability of information systems. These standards are classified in two ways: information security standards and information security management standards. Information security encompasses standards and frameworks that focus on security measures such as the ISO/IEC27000 series and NIST.

The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other tools. In order to provide accurate information for long-term research that anticipates technology developments and future challenges, NIST offers more than a thousand standard reference materials [14–17].

The choice of appropriate cybersecurity standards is crucial in protecting an information resource [6, 7, 8]. These components have an exhaustive list of controls that can be used as a benchmark for protecting information systems. Thus, the format of control channel protection is selected based on the tasks, structure, and requirements.

The NIST STS methodology applied in testing statistical properties [18] has become widespread,

and therefore this test suite was chosen to verify the developed methods.

Analysis of recent research and publications. The conceptual foundations for constructing low-resource stream ciphers are considered in [1, 19]. These research papers present applied aspects of using CET operations. The results of the impact the CET encryption technologies have on the identification and evaluation of ways to improve the already known cryptographic algorithms and build new ones are studied in the works [2, 3].

The classification of CET operations by the number of operands into one-operand, two-operand, three-operand, etc. is given in [4, 5]. To build cryptographic systems, it is proposed to use multi-operand CET operations. Technologies used to construct two-operand operations are given in [3, 4, 5].

The authors [2] suggest using a discrete casual representation of models of elementary functions and CET operations, including information-driven CET operations.

Pseudorandom sequence generators are used in various fields of knowledge such as information and communication technologies [12, 18], information security in networks and systems [13, 14, 15], mathematical modeling, information resource processing, generation of pseudorandom variables, etc. In the vast majority of cryptographic protocols, random numbers are used as input at some points [16] or as a key in streaming encryption systems [17].

The main results for the study of operations of low-resource cryptographic systems and the results for cryptographic transformations are laid out in the research papers [1–5, 19].

The purpose of the article is to evaluate the statistical properties of the results for CET encryption of information-driven permutation operations.

Summary of the main material. Various software systems are used to study cryptographic algorithms and evaluate the quality of PRS generators, among which the following deserve special attention: the DIEHARD Statistical RNG Tests, the NIST Statistical Test Suite (USA) [18], and the system for evaluating the statistical security of PRN generation algorithms and cryptoalgorithms.

The battery of DIEHARD statistical tests for measuring the quality of a random number generator has its drawbacks, namely the test parameters are rigidly fixed; there is a lack of a help desk and a methodology for interpreting the processing results; some tests have no substantive justification [18].

Within the framework of the AES (Advanced Encryption Standard) project, NIST [National Institute of Standards and Technology] engineers developed the NIST Statistical Test Suite (STS) and proposed a methodology for statistical testing of pseudorandom number generators for use in cryptographic information security, which, according to experts in this field, currently best meets the requirements of all stakeholders [16, 17, 18].

The simplicity of the discrete-casual representation of models of elementary functions of information-guided permutations has provided a simple representation of models of one-operand CET operations of information-guided permutations. For the first time, the basic group of one-operand information-driven CET operations of permutations contains only symmetric operations, each of which implements a direct and an inverse transformation.

The main hypothesis of the study is that it is possible to combine one-operand information-driven permutation CET operations into two-operand operations based on the use of discrete-casual models.

The proof of the hypothesis involves the use of discrete-casual models of elementary information-driven permutation functions to build models of one-operand and two-operand CET operations. The methods of discrete mathematics, set theory and situational management were used to establish the relationships between the models of one-operand CET operations in the tuple of a two-operand NET operation and its modification.

The design of lightweight ciphers involves reducing the complexity of information transformation algorithms if the preservation of their cryptographic strength is desired. Among the three-bit elementary functions on the basis of which CET operations are built, one of the simplest in terms of hardware implementation is the elementary functions of information-driven permutations [2]. Their functional complexity is similar to the complexity of modulo 2 bit addition (Figure 1).

The low complexity of implementing elementary functions of information-driven permutations ensures the feasibility of their application in low-resource stream encryption systems. Let us investigate the possibility of constructing discrete-casual models of elementary functions, one- and two-operand CET operations of information-driven permutations.

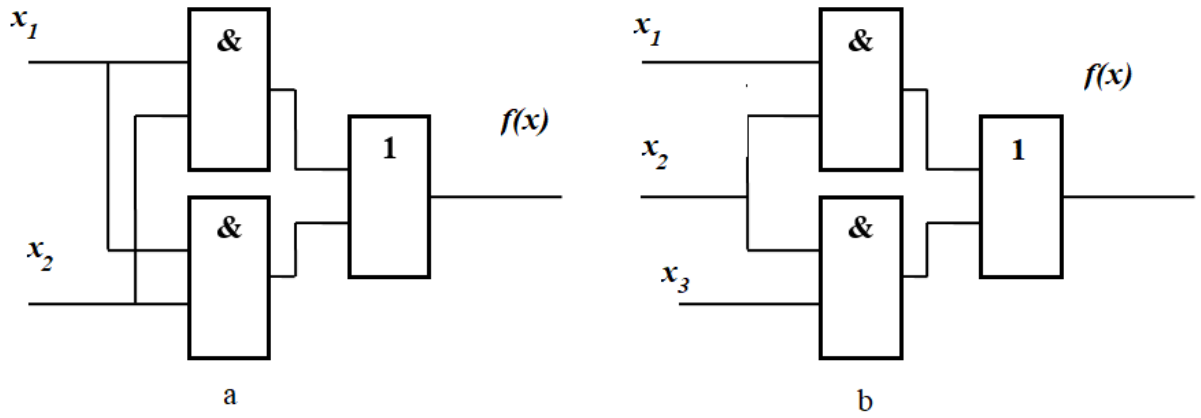

Figure 1 – Functional diagrams for the implementation of elementary functions of modulo 2 addition (a) and information-driven permutation (b) (*developed by the authors*)

The discrete-casual model is a casual combination of three discrete functions [2]:

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

where $f_2(x)$ is control function; $(f_1(x))$ and $(f_3(x))$ are the permutation function 1 and the permutation function 2 correspondingly; in case of $f_2(x)$ the permutation function 1 $(f_1(x))$ is performed; otherwise the permutation function 2 $(f_3(x))$ is implemented.

The elementary information-driven permutation function presented in Figure 1, according to (1), can be described by the model:

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

To improve the methods of synthesis of elementary functions and information-driven CET operations of permutations, the following properties of the discrete-casual model are required (1):

– inversion of the result for the control function implementation will lead to a swapping of the permutation functions:

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

– inversion of the results for the implementation of the permutation functions will lead to the inversion of the implementation of such a model:

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

Using the model (2), we can construct all elementary information-driven permutation functions.

1. Based on permutations of three discrete functions, i.e. $f_1(x) = x_1$, $f_2(x) = x_2$ and $f_3(x) = x_3$, six discrete-casual models can be built: $f(x) = (x_1)(x_2)(x_3)$; $f(x) = (x_1)(x_3)(x_2)$; $f(x) = (x_2)(x_1)(x_3)$.

2. Contingent on each model built by inversion of the permutation functions, four discrete-case models can be constructed: $f(x) = (x_1)(x_2)(x_3)$; $f(x) = (\overline{x_1})(x_2)(x_3)$; $f(x) = (x_1)(x_2)(\overline{x_3})$; $f(x) = (\overline{x_1})(x_2)(\overline{x_3})$ …

3. Due to the second property, the obtained discrete-case models can be divided into direct and inverse ones.

The results for the synthesis of models of elementary information-driven permutation functions are shown in Table 1.

Table 1 – A set of synthesized models of elementary information-driven permutation functions *(developed by the authors)*

Elementary functions of information-driven permutations			
direct		inverse	
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	$f(x) = (x_3)(x_2)(x_1)$

The constructed group of discrete-casual models of elementary functions of information-driven permutations allows proceeding to the modeling of one-operand CET operations of information-driven permutations.

Let us check the possibility of detecting the statistical properties of the results for the matrix cryptographic transformation of a non-random monotonically increasing sequence with a repetition cycle of 256 bytes, which contains the codes of the numbers 0, 1, 2, ..., 255.

The algorithm for forming a sequence based on information-driven permutation CET operations is shown in Figure 2. It presents the complete processing cycle for information-driven CET operations.

The sequence was tested based on information-driven permutation CET operations using the NIST STS.

The cumulative results of testing the sequence based on information-driven permutation CET operations with a 256-byte repetition cycle by the NIST STS are presented in Table 2.

The test results showed that the method of information protection based on CET encryption of information-driven permutation operations has passed the comprehensive control according to the NIST STS methodology.

Let us check the statistical properties of the results for cryptographic transformation based on information-driven CET operations on the example of electronic information resources.

A statistical portrait of the software implementation of the sequence formation algorithm based on information-driven permutation CET operations with a 256-byte repetition cycle is shown in Figure 3.

Taking into account the software implementation of the information security method, the generated pseudorandom sequences were tested with the NIST STS. The analysis of the test results made it possible to conclude that the proposed method of sequence formation based on information-driven permutation CET operations is suitable for use in systems for protecting information resources of the weapons and military equipment system.

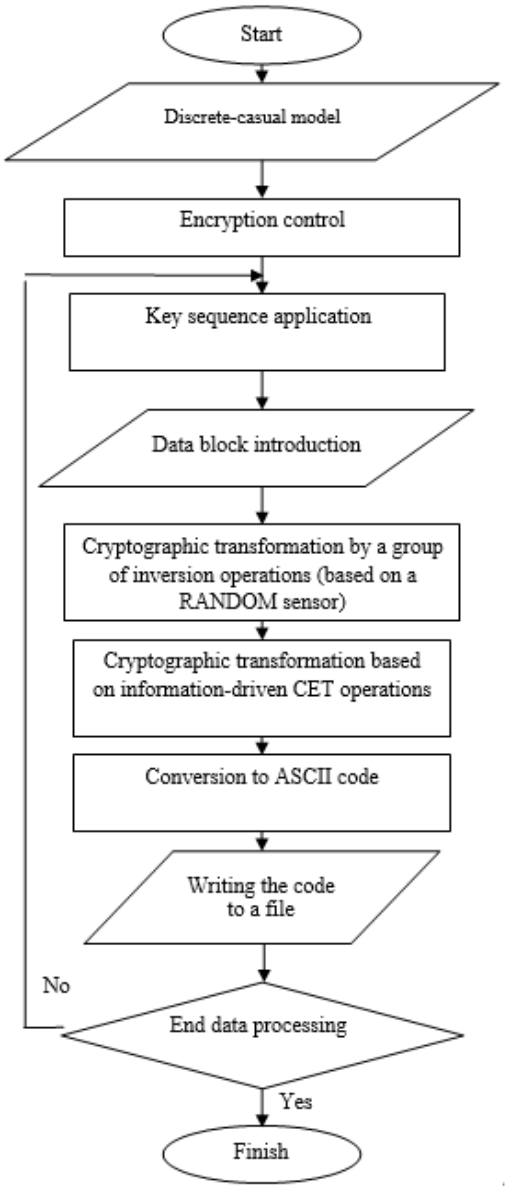

Figure 2 – Algorithm for sequence formation based on information-driven permutation CET operations *(developed by the authors)*

Table 2 – The summary of test results *(developed by the authors)*

Generator	Number of the tests passed	
	99 % consecutive	96 % consecutive
Cryptographic transformation based on information-driven CET operations	136 (71.9 %)	188 (99.5 %)

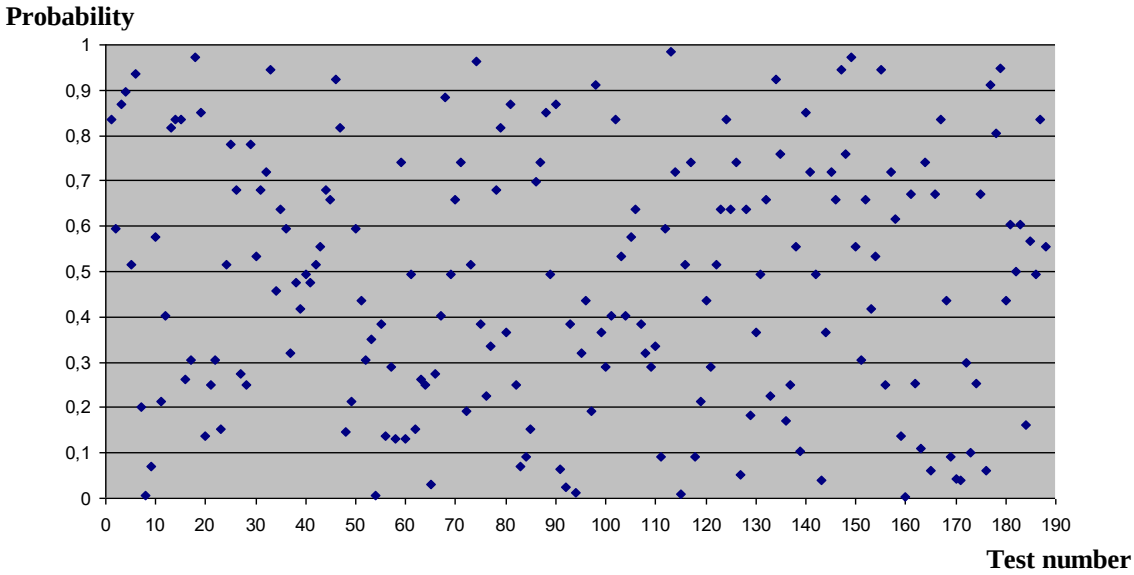

Figure 3 – Statistical portrait of the software implementation of the sequence formation algorithm based on information-driven permutation CET operations *(developed by the authors)*

As can be seen from the results, the sequence under study has undergone comprehensive control according to the NIST STS methodology [18].

Conclusions

The article evaluates the statistical properties of encryption results based on information-driven permutation CET operations on the basis of generalization of the obtained results.

It is possible to increase the speed of the information security system based on information-driven permutation CET operations by controlling the encryption process. A variant of the algorithm for forming a sequence based on information-driven permutation CET operations is shown in Figure 2.

The practical implementation of the algorithm for forming a sequence based on information-driven permutation CET operations depends on the requirements for the development of cryptographic protection systems for information resources.

The implementation of information-driven permutation CET operations based on a pseudorandom (gamma) sequence meets the requirements of the NIST Statistical Test Suite.

Direction to further research is construction of groups of non-commutative two-operand information-controlled CET operations of permutation for use in promising scenarios of low-resource stream encryption.

References

1. Rudnytskyi V., Lada N., Kuchuk G. & Pidlasyi D. (2024). Architecture of CET-operations and stream encryption technologies. Cherkasy : R. V. Ponomarenko. Retrieved from: https://surl.li/hfzghl (accessed 14 October 2024) [in English].

2. Rudnytskyi V., Lada N., Pochebut M., Melnyk O. & Tarasenko Ya. (2023). 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), October 13–15, 2023, Athens, Greece, pp. 1–6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416546 [in English].

3. Babenko V., Melnyk O., Melnyk R. (2013). *Klasyfikatsiia tryrozriadnykh elementarnykh funktsii dlia kryptohrafichnoho peretvorennia informatsii* [Classification of three-bit elementary functions for cryptographic transformation of information]. *Bezpeka informatsii,* vol. 19, no. 1, pp. 56–59. Retrieved from: https://surli.cc/duunzv (accessed 14 October 2024) [in Ukrainian].

4. Rudnytskyi V. M., Larin V. V., Melnyk O. H., Pidlasyi D. A. (2023). *Dyskretno-kazualne predstavlennia modelei elementarnykh funktsii i SET-operatsii* [Discrete-casual presentation of models of elementary functions and CET operations]. *Systemy upravlinnia, navihatsii ta zviazku,* no. 4,

pp. 96–101. DOI: https://doi.org/10.28925/2663-4023.2024.23.616 [in Ukrainian].

5. Rudnytska Yu. V., Rudnytskyi S. V. (2022). *Modeliuvannia symetrychnykh operatsii kryptohrafichnoho koduvannia* [Modeling of symmetric cryptographic coding operations]. Proceedings of the 10th International scientificand practical conference *"Problemy informatyzatsii"* (Ukrain, Cherkasy – Baku – Belsko-Biala – Kharkiv, November 24–25, 2022). Cherkasy : ChDTU; Baku : VA ZS AR; Belsko-Biala : UTiHN; Kharkiv : NTU "KhPI", vol. 2, p. 10 [in Ukrainian].

6. Dhaou I. B., Skhiri H., Tenhunen H. (2017). 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, pp. 1–9 [in English].

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

8. Choi J. (2017). Physical Layer Security for Channel-Aware Random Access with Opportunistic Jamming. IEEE Trans. Inf. Forensics Secur., 12, pp. 2699–2711 [in English].

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

10. Gergely A. M., Crainicu B. (2017). 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, pp. 1–6 [in English].

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

12. Benedetti R., Andreano M. S., Piersimoni F. (2019). Sample selection when a multivariate set of size measures is available. Stat. Methods Appl., 28, pp. 1–25 [in English].

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

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

15. Khan A., Bryans J. and Sabaliauskaite G. (2022). 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. Springer [in English].

16. Taherdoost H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards. A Review and Comprehensive Overview. *Electronics*, no. 11 (14), p. 2181 [in English].

17. Hijji M. and Alam G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, no. 22, p. 86 [in English].

18. Rukhin A., Soto J., Nechvatal J. et al. (2022). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Retrieved from: https://surl.lu/jsuhvq (accessed 14 October 2024) [in English].

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

20. Shuhurov O. S. (2007). Rozvytok viiskovykh nazemnykh robotyzovanykh system v konteksti novykh kontseptsii upravlinnia: perspektyvy Ukrainy [Development of military ground robotic systems in the context of new concepts of management: perspectives of Ukraine]. *Stratehichni priorytety*, no. 4, pp. 198–205. Retrieved from: https://surl.li/pifinl (accessed 14 October 2024) [in Ukrainian].

The article was submitted to the editorial office on 15 February 2025

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.

На підґрунті узагальнення отриманих результатів розроблено метод криптографічного перетворення на основі СЕТ-операцій, керованих інформацією.

Запропоновано структуру системи захисту інформаційного ресурсу на основі криптографічного перетворення у разі застосування СЕТ-операцій, керованих інформацією, і розроблено функціональні схеми пристроїв реалізації елементарних функцій.

Результати тестування показали, що розроблений метод захисту інформації на основі СЕТ-операцій перестановок, керованих інформацією, у межах контрольного діапазону за методикою NIST STS. Це дало змогу дійти висновку, що запропонований метод криптографічного перетворення на основі СЕТ-операцій, керованих інформацією, є прийнятним для використання у системах озброєння та військової техніки.

Побудовано дискретно-казуальні моделі елементарних функцій перестановок, керованих інформацією. Установлено властивості цих моделей, які дали змогу спростити метод їх синтезу.

Було використано лише двохоперандні СЕТ-операції базової групи операцій, які отримані за результатами експерименту. Таке обмеження зумовлене наявністю можливості побудови повної групи моделей одноопераднних СЕТ-операцій перестановок, керованих інформацією, з моделей одноопераднних СЕТ-операцій базової групи.

Показано, що генератори псевдовипадкових послідовностей є найважливішими елементами будь-якої системи захисту, надійність роботи яких переважно визначається саме властивостями використовуваних генераторів. Стійкі псевдовипадкові послідовності, які є за своєю сутністю обмеженими, мають практично всі властивості реалізацій істинно 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.*

Rudnytskyi Volodymyr – Doctor of Technical Sciences, Professor, Chief Researcher State Scientific Research, Institute of Armament and Military Equipment Testing and Certification
https://orcid.org/0000-0003-3473-7433

Larin Volodymyr – Doctoral Candidate, Candidate of Technical Sciences, Associate Professor, State Scientific Research, Institute of Armament and Military Equipment Testing and Certification
https://orcid.org/0000-0003-0771-2660

Nikorchuk Andrii – Doctoral Candidate, Candidate of Technical Sciences, Associate Professor, National Academy of the National Guard of Ukraine
https://orcid.org/ 0000-0003-2683-9106