http://doi.org/10.35784/iapgos.916

# THE GENERATING RANDOM SEQUENCES WITH THE INCREASED CRYPTOGRAPHIC STRENGTH

**Volodymyr Korchynskyi, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov**
Odessa National Academy of Telecommunication named after O.S. Popov, Institute of Radio, Television and Information Security, Department of Information Security, Odessa, Ukraine

***Abstract.*** *Random sequences are used in various applications in construction of cryptographic systems or formations of noise-type signals. For these tasks there is used the program generator of random sequences which is the determined device. Such a generator, as a rule, has special requirements concerning the quality of the numbers formation sequence. In cryptographic systems, the most often used are linearly – congruent generators, the main disadvantage of which is the short period of formation of pseudo-random number sequences. For this reason, in the article there is proposed the use of chaos generators as the period of the formed selection in this case depends on the size of digit net of the used computing system. It is obvious that the quality of the chaos generator has to be estimated through a system of the NIST tests. Therefore, detailed assessment of their statistical characteristics is necessary for practical application of chaos generators in cryptographic systems. In the article there are considered various generators and there is also given the qualitative assessment of the formation based on the binary random sequence. Considered are also the features of testing random number generators using the system. It is determined that not all chaos generators meet the requirements of the NIST tests. The article proposed the methods for improving statistical properties of chaos generators. The method of comparative analysis of random number generators based on NIST statistical tests is proposed, which allows to select generators with the best statistical properties. Proposed are also methods for improving the statistical characteristics of binary sequences, which are formed on the basis of various chaos generators.*

**Keywords**: dynamic chaos, generator, sequence, encryption

## GENEROWANIE SEKWENCJI LOSOWYCH O ZWIĘKSZONEJ SILE KRYPTOGRAFICZNEJ

***Streszczenie.*** *Sekwencje losowe wykorzystywane są do tworzenia systemów kryptograficznych lub do formowania sygnałów zakłócających. Do tych zadań wykorzystywany jest generator sekwencji losowych, który jest urządzeniem deterministycznym. Taki generator z reguły ma specjalne wymagania dotyczące jakości tworzenia sekwencji liczbowej. W systemach kryptograficznych najczęściej stosuje się generatory liniowo-przystające, których główną wadą jest krótki okres formowania pseudolosowych sekwencji liczbowych. Z tego powodu w artykule zaproponowano użycie generatora chaotycznego, jako że okres próbkowania w tym przypadku zależy od rozmiaru siatki bitowej w używanym systemie obliczeniowym. Oczywistym jest, że należy oszacować jakość generatora chaotycznego za pomocą systemu testów NIST, dlatego też do praktycznego zastosowania generatorów chaotycznych w systemach kryptograficznych wymagana jest szczegółowa ocena ich cech statystycznych. W artykule rozważono różne generatory, a także podano ocenę jakościową procesu formacji na podstawie losowej sekwencji binarnej. Rozważano również funkcje testowania generatorów liczbowych przy użyciu systemu. Stwierdzono, że nie wszystkie generatory chaotyczne spełniają wymagania testów NIST. W artykule zaproponowano metody poprawy właściwości statystycznych generatorów chaotycznych, tak jak również metodę analizy porównawczej generatorów liczb losowych, która oparta jest na testach statystycznych NIST, i która pozwala wybrać generatory o najlepszych cechach statystycznych. Przedstawiono także metody poprawy właściwości statystycznych sekwencji binarnych, które powstają na podstawie różnych generatorów chaotycznych.*

**Słowa kluczowe:** chaos dynamiczny, generator, sekwencja, szyfrowanie

## Introduction

The protection of the transmitted information from unauthorized access is carried out at different levels of OSI models [2, 4, 6] by means of cryptographic systems and noise-like signals. The confrontation between cryptography and cryptanalysis allows to conclude that the reliability of the cryptographic system decreases over time and its compromise becomes apparent. Therefore, it is possible to guarantee the high cryptographic stability of the encryption systems by their constant improvement.

Another purpose of random numbers is to expand the spectrum of digital signals to form noise-like signals, on which based are various implemented indicators of transmission stealth. It is obvious that the cryptographic strength of encryption systems, and the level of energy and structural secrecy of noise-like signals are affected by the quality of the used random number generators [5, 8]. It is known [8] that in cryptographic systems, as a rule, used are the linear congruent generators. The main disadvantage of such generators is a short period of formation of random numerical sequences.

The implementation of the dynamic chaos phenomenon [1, 4, 7] into the field of information and communication technologies not only opened new prospects for the synthesis of signal structures, which are providing high potential stealth of transmission, but also expanded the possibilities for developing effective cryptocoding systems. For this reason, it is expedient to improve the methods for generating random sequences and this substantiates the relevance of this research. Therefore, the aim of this work is to develop methods for the formation of pseudorandom sequences based on dynamic chaos with improved statistical characteristics and increased cryptographic strength.

## 1. The features of testing random sequences

The random sequences based on dynamic chaos should satisfy the corresponding statistical properties of the generated processes. Dynamic chaos [7] has all the basic properties of a random process and is an irregular, aperiodic change in the state of a nonlinear dynamic system. An insignificant change in the initial parameters of the chaos generator leads to a significant change in the values of the generated oscillations, which makes it possible to form different trajectories of the chaotic process. This property allows one to create almost unlimited number of random sequence combinations of various lengths.

For cryptographic tasks and noise-like signals, it is advisable to use program generators with a uniform distribution law of numbers [3]. Such generators are implemented in accordance with a certain algorithm, according to which each successive random number is calculated from the previous one. This method of forming a sequence has the following advantages:

1) the selection of a sample of numbers with tested statistical properties, which provides the necessary stability of the numbers generation and does not require regular testing of the sequence;
2) the repeated reproduction of a numerical sequence from the desired position;
3) the minimum number of operations that is necessary for the formation of each member of the numerical sequence;
4) the computational process does not occupy large amounts of memory;
5) the sequence period must be no less than the specified process.

The research of generators with a uniform distribution law [8] shows that the search for samples with the required quality indicators is a difficult task and requires rather large laborious calculations. There are various statistical criteria for checking

random and pseudo-random number generators [2]: criteria $\chi^2$ (Pearson), Kolmogorov-Smirnov criteria, Student criteria, and others. The most convenient and universal is the criteria $\chi^2$, the advantages of which are independent of the distribution of a random variable.

As noted in [2], using statistical criteria, you can implement such verification tests as distribution check (test frequencies), series check (test pairs), intervals check (testing intervals), combinations check (poker test) etc. For the task of testing random numbers, the National Institute of Standards and Technologies (NIST) has developed 16 special tests: the seriality test (Runs Test); test for maximum batch size; matrix-rank test (Random Binary Matrix Rank Test); spectral test; test with non-overlapping non-periodic patterns (Nonoverlapping (Aperiodic) Template Matching Test); test for overlapping periodic patterns (Overlapping (Periodic)); universal statistical test (Maurer's Universal Statistical Test); comprehensive test Lempel-Ziv (Lempel-Ziv Complexity Test); linear test (Linear Complexity Test); serial test (Serial Test); with – approximate entropy test (Approximate Entropy Test); summing test (Cumulative Sum (Cusum) Test); random deviation test (Random Excursions Test and Random Excursions Variant Test).

The method of comparative analysis of random sequences generators requires the following actions:

1) with the help of NIST tests, sample testing of the number generators under study is carried out;
2) counting the number of values that went beyond the limits of the confidence interval;
3) according to the number of internal local deviations Z, an analysis of the quality indicators of generators, for which the Z values are ranked in ascending order.

## 2. Generation and testing of binary sequence based on the dynamic chaos

Consider the method of improving the qualitative realizations of chaotic oscillations [7]. To solve the experiment, we consider several discrete mappings in chaos generators [5]:

1) static

$$x_{n+1} = a(1-|1-2x_n|^l) \tag{1}$$

where $x_0 = 0.8$, $a = 0.9$, $l = 0.8$;

2) logistic

$$x_{n+1} = ax_n(1-x_n) \tag{2}$$

where $x_0 = 0.9$, $a = 3.9$;

3) cubic

$$x_{n+1} = (1-4a)x_n + 4ax_n^3 \tag{3}$$

where $x_0 = 0.5$, $a = 0.92$;

4) shear

$$x_{n+1} = ax_n \bmod 1 \tag{4}$$

where $x_0 = 0.8$, $a = 3.0$.

For generators (1-4), Fig. 1 shows the graphs of dependence $P(\chi^2)$ on the values $n$, which are calculated in the process of generating numbers through the interval $\Delta n = 2 \cdot 10^3$ for the implementation lengths of 450,000 values.

The graph of the dependence $P(\chi^2)$ on the values $n$ of the sequence for the length $\overline{y_n}$ of the implementation of 450,000 values is shown in Fig. 2 (a). In Fig. 2 (b) there is the graph of the dependence $P(\chi^2)$ on the values $n$ of the sequence $\overline{z_n}$.

From the analysis of the dependency graphs $P(\chi^2)$, we see that the bottom line with the accepted criterion, as the base random generator, should be taken by the generator sequence $\overline{z_n}$. We can assume that the implementation of pseudorandom numbers based on such a generator is a random distribution. As shown in [1], the sequence $\overline{z_n}$ represents a noise signal. Thus, the noise signal can be considered a truly casual process, for the purpose of generating random numbers. By applying a sign function $signx$, which is conditioned as $signx = 1$ at $x \geq 0$ and $signx = -1$ at $x < 0$, we will form a binary sequence based on the chaos generator.

The resulting sequence $\ddot{z}_n$ of 450000 bits is initially generated to form a desired length through the dilution procedure. For example, by double-thinning with a different step, we will generate a binary sequence 20000 bits long and check it randomly with a frequency test. This test is based on the equality of frequencies "1" and "-1" in a truly random binary sequence.

If $X$ marks the amount of "1" i "−1" in binary sequences, then in the experiment under consideration

$$X = \sum_{i=0}^{20000} \ddot{z}_i = -1 \tag{5}$$

indicates that the frequency test of a random binary sequence has been successfully completed.

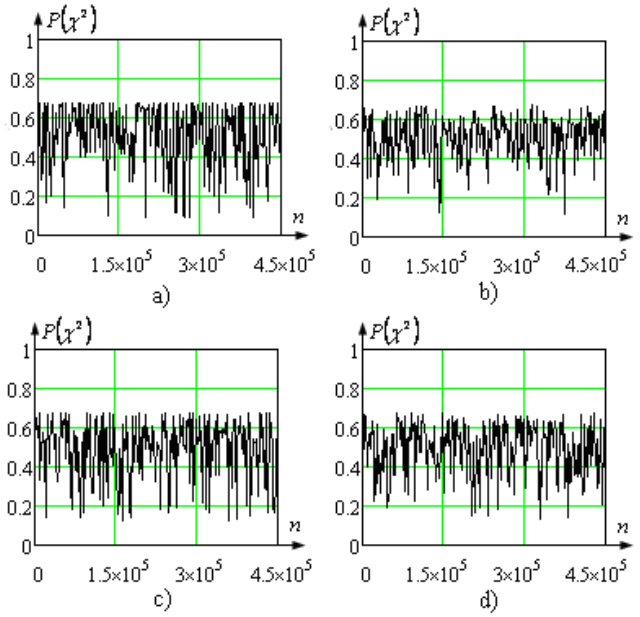



*Fig. 1. The graphs of dependency P($\chi^2$) from the quantity of numbers n generators of discrete mappings: static (a), logistic (b), cubic (c) and shift (d)*

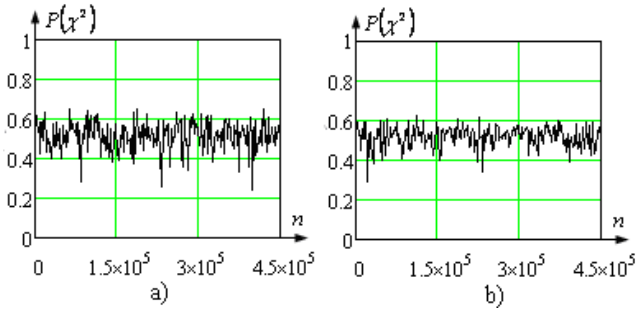



*Fig. 2. The graphs of dependency P($\chi^2$) from the quantity of numbers n to (a) and after (b) mixing*

Thus, we can conclude that the chaos generator $\overline{z_n}$ is the ideal basis for the formation of the random binary sequence that provides reproduction and the required length of a random sequence. The application of such sequences in transmission algorithms will increase the noise immunity, structural and informational concealment of signal structures in the confidential communication systems.

With the help of the various NIST system tests, there can be considered the process of statistical evaluation $P(\chi^2)$ of binary sequences formed on the basis of chaos generators (1-4). Fig. 3 shows the values $P(\chi^2)$ that depends on the NIST system tests. Based on the results of values $P(\chi^2)$ deviations in the zone of the

confidence interval, it can be concluded that not all samples of chaos generators meet the requirements of the NIST test system. For example, chaos generators with a logistic (Fig. 4) and cubic (Fig. 5) mapping, as well as a chaos generator with a shift type display (Fig. 6), do not pass all tests on randomness, as a series of values obtained $P(\chi^2) < 0.05$. Satisfactory results for NIST tests were obtained for a power chaos generator (Fig. 3).

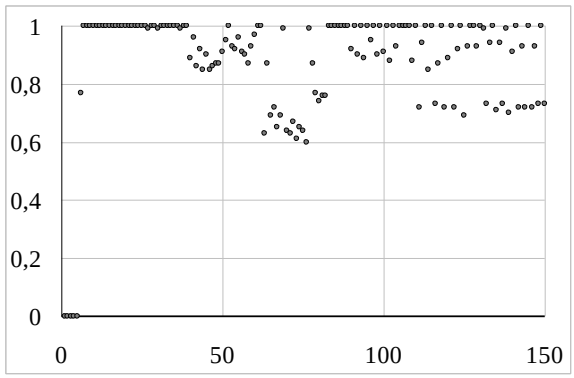



*Fig. 3. The results of testing the power chaos generator*

To increase the stability of the statistical characteristics of a binary sequence, it was proposed to use several chaos generators. For this purpose, the XOR operation was used to form the final binary sequence. Fig. 7 shows the results of testing such sequence, which is formed on the basis of a shift type generator and a cubic generator. The test results show that the quality of the obtained sample has significantly improved, since most of the tests are in the zone of the confidence interval, i.e. $P(\chi^2) > 0.05$.

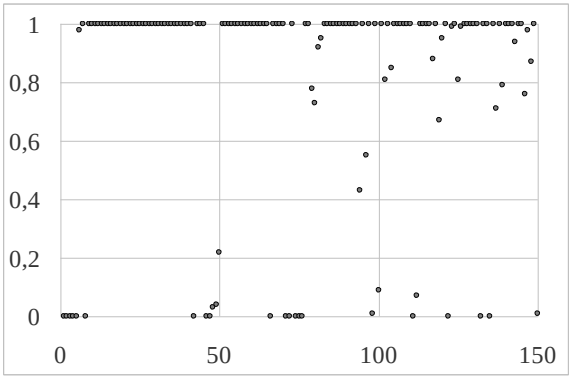



*Fig. 4. The results of testing the chaos generator with the logistic display*

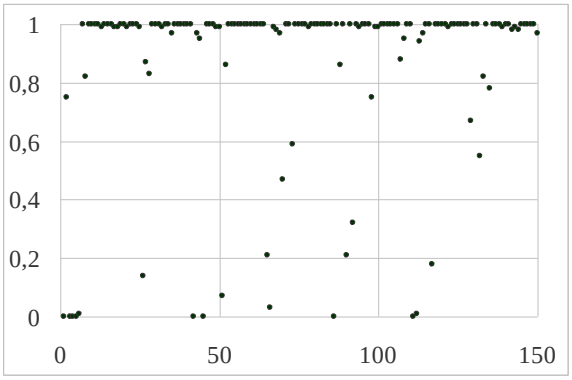



*Fig. 5. The results of testing the chaos generator with a cubic map*

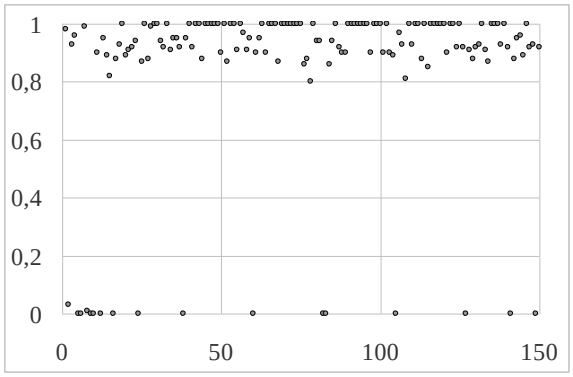



*Fig. 6. The results of testing the chaos generator with mapping type shift*

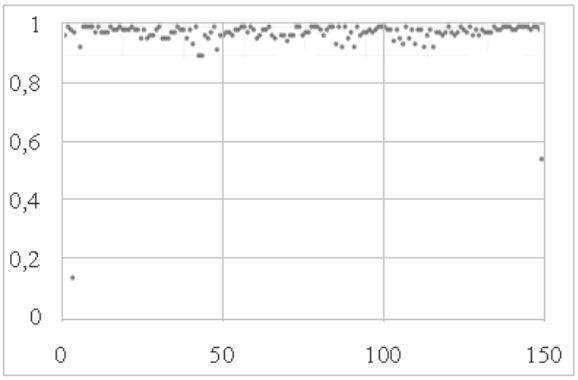



*Fig. 7. The results of testing the sequence generated on the basis of a shift type generator and a cubic generator*

## 3. The generation of sequences with increased cryptographic strength

The cryptographic resistance of encryption systems depends directly on the degree of randomness of the used numbers sequence. Provided that the random sequence of the generator satisfies the tests using statistical tests, then it can be considered random. However, this is not sufficient enough condition to ensure the cryptographic strength of the random number generation algorithm. It is considered that the sequence is cryptographically safe if it has the property of unpredictability of the next generated number. As a rule, a random number generator has this property.

Let us consider the algorithm for generating random number sequences with increased cryptographic strength. The essence of the method is as follows:

1) using the first chaos generator, forming the set of $N$ random numbers in the interval ]0;1[:
$$x_1, x_2, x_3, \ldots, x_N \quad (6)$$
2) the interval from 0 to 1 is divided into $z$ equal parts (for example, $z = 2$, or $z = 3$, or $z = 4$, etc.);
3) the first subset is selected from $z$ numbers, for example, with $z = 3$ selected are numbers $x_1$, $x_2$, $x_3$, and $x_1$ corresponds to the 1st interval, $x_2$ – 2nd interval, $x_3$ – 3rd interval;
4) using the second generator, random number $y_j$ is formed in the interval ]0;1[;
5) if $0 < y_j < 0.33$, then selected is the number $x_1$, if $0.33 < y_j < 0.66$, then $x_2$, if $0.66 < y_j < 1$, then $x_3$;

If $0.33 < y_1 < 0.66$, then selected is number $x_2$. Similarly, the next number is selected from the subset $\{x_4, x_5, x_6\}$. If $0.66 < y_2 < 1$, then selected is number $x_6$. When $0 < y_3 < 0.33$ the selected number is $x_7$, etc.

The process of the random sequence generation when $z = 3$ is shown in Fig. 8.

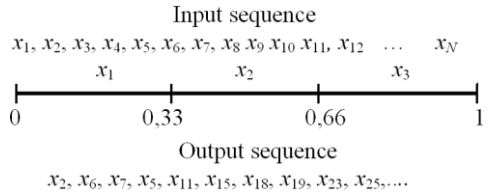



*Fig. 8. The process of generating random sequence when z = 3*

Thus, as the result obtained will be a random sequence

$$x_v, x_{z+v}, x_{2z+v}, x_{3z+v}, \cdots; \quad (7)$$

where $v = 1 \ldots z$ – the number of the selected numeric in the subset.

Next, the sequence (6) is converted into a binary sequence, taking into account the system of the following conditions: $x_i < 0.5$, then $s_i = 0$; $x_i \geq 0.5$, then $s_i = 1$.

Obviously, the degree of randomness of the generated numbers depends on the amount of the $Z$ numbers in the used subset.

## 4. Conclusion

The results of the research have shown that not all chaos generators fully satisfy the requirements of the NIST test system. It means that the use of chaos generators for the formation of binary sequences may be limited. The chaos generators with logistic (2) and cubic (3) mappings, and also the chaos generators with a shift type display (4), did not pass the tests for randomness in full, because the number of values $P(\chi^2)$ went beyond the limit of the confidence interval.

It has been proposed to improve the qualitative characteristics of the binary sample due to the XOR operation and the use of several source sequences formed using chaos generators. For the task of the experiment there were used a shift type generator and a cubic generator, which showed unsatisfactory results during testing.

The sample obtained while using XOR received higher marks than while conducting tests using the NIST system (Fig. 5), because for the most tests the value $P(\chi^2)$ is in the zone of the confidence interval. It can be supposed that the use of the large number of chaos generators (2-4) significantly stabilizes the statistical characteristics of a binary sample. However, the number of operations for the formation of one bit will increase. This must be considered when constructing the source of a binary sequence.

Proposed is the algorithm for increasing the cryptographic stability of the generator due to the uncertainty of the number appearance in a random sequence. It is achieved by the use of subsets from $Z$ numbers over the entire interval of the formation sequence. With the increasing $Z$, the cryptographic strength of the algorithm for generating random sequence of numbers rises. However, more implementation is required.

## References

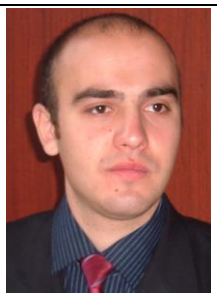
[1] Ipatov V. P.: Broadband Systems and Code Separation of Signals. Principles and Applications. Tech-Nosfera, Moscow 2007.
[2] Knuth D.: The Art of Programming. Williams, 2000.
[3] Korchynskyi V., Filkin K.: Analysis of Models of Primary Sensors of Pseudo-random Numbers. Proc. of Semin. young science students and students of the Advanced Telecommunications Technology and Information Technology, 2007, 20–24.
[4] Korchynskyi V.: A Method of Increasing the Secrecy of Transmission by Timer Signals in Communication Systems with Code Division of Channels. Visnik of the V. Dahl East Ukrainian National University 15(204)/2013, 93–99.
[5] Korchynskyi V: A Model of a Noise Signal for Transmitting Confidential Information. Bulletin of NTU "KhPI" 11(985)/2013, 89–94.
[6] Kupriyanov A. I., Sakharov A.: Theoretical Foundations of Electronic Warfare, University Book, Moscow 2007.
[7] Kuznetsov S. P.: Dynamic Chaos. Physico-mathematical literature, Moscow 2006.
[8] Zakharchenko M., Korchynskyi V.: Transmission Secrecy in Communication Systems with Chaotic Signals Measuring and enumerated technology in technological processes. International science and technology technical magazine 3/2013, 161–164.

**D.Sc. Volodymyr Korchinskyi**
e-mail: vladkorchin@ukr.net

Associate Professor, Department of Information Security and Data Transmission.
In 2007, he defended a dissertation on the specialty "Telecommunication systems and networks". In 2012, he was awarded the academic title of Associate Professor of the Department of Information Security and Data Transmission at Odessa National Academy of Telecommunication named after O.S. Popov. In 2014, he defended a doctoral dissertation on the specialty "Information Security Systems".

http://orcid.org/0000-0003-3972-0585

**Ph.D. Vitalii Kildishev**
e-mail: kildishev@ukr.net



Associate Professor, Department of Information Security and Data Transmission.
In 2008, he defended a dissertation on the specialty "Telecommunication systems and networks". In 2013, He was awarded the academic title of Associate Professor of the Department of Information Security and Data Transmission. The field of his scientific interests covers the enhancing security of information transmission in telecommunication systems based on integrated processing methods.

http://orcid.org/0000-0002-7121-4060

**Ph.D. Oleksandr Riabukha**
e-mail: ryabukha@gmail.com

Senior Lecturer, Department of Information Security and Data Transmission.
In 2012, he defended a dissertation on the specialty "Telecommunication systems and networks".
The field of his scientific interests covers the enhancing security of information transmission in telecommunication systems based on integrated processing methods. He is the author of over 20 scientific papers in the field of communication and information protection.

http://orcid.org/0000-0001-7402-0395

**M.Sc. Oleksandr Berdnikov**
e-mail: berdnikov2000@gmail.com

In 2001, he graduated from the department of multichannel telecommunications ONAT them. A.S. Popova. Since 2017, He is studying at the graduate school of the Odessa National Academy of Communications named after A.S. Popov, specialty 125 – Cybersecurity. The field of his scientific interests covers the protection of transmitted information from unauthorized access based on dynamic chaos.
He have authored over 7 scientific papers in the field of communication and information protection.

http://orcid.org/0000-0003-0058-9997

*otrzymano/received: 15.11.2019* *przyjęto do druku/accepted: 15.02.2020*