Обґрунтовано шляхи підвищення продуктивності генерації випадкових послідовностей, що утворені від фізичних джерел, для систем захисту інформації. Це потрібно тому, що на сьогоднішній день відбувається бурхливе зростання технологічних можливостей та швидкісних показників реалізації різноманітних інформаційних сервісів та додатків, що потребує спільнота. Одним з головних питань безпечного використання цих сервісів є гарантування інформаційної безпеки, яка вимагає використання ефективних швидкодіючих систем захисту інформації та високопродуктивної генерації послідовностей випадкових даних. При проведенні досліджень з метою підвищення продуктивності здійснено аналіз особливості перетворення реальних шумових процесів з врахуванням їх нестаціонарності та відхилень від розподілу ймовірностей. Запропоновано шляхи вдосконалення методів аналого-цифрового перетворення з оптимізацією шкали квантування динамічного діапазону та кроку дискретизації шумового процесу в часі. З метою вирівнювання статистичних характеристик розглянуто можливість використання методів обробки, які підвищують її статистичну якість з економією швидкісних втрат. Це метод вибірки рівноймовірних комбінацій (von Neumann – Elias – Рябко – Мачикиної) та метод кодової оброки (Santha – Vazirani), які завдяки розширення коду забезпечують певну ефективність та полягають в перетворенні послідовності: в першому з використанням рівноймовірних комбінацій з відкиданням непотрібних даних, в другому без їх відкидання з можливістю лінійного перетворення. З метою оптимізації параметрів перетворення на обох етапах генерації та адаптації цих параметрів до особливостей і змінності характеристик перетворюваних випадкових процесів запропоновано використання зворотних зв'язків виходів перетворювачів з попередніми елементами перетворення. Коригування вказаних параметрів має здійснюватись під час генерації за результатами статистичного аналізу виходів етапів перетворення. Отримані результати є досить важливими, оскільки їх реалізація в сучасних системах захисту інформації дозволить гарантоване забезпечення інформаційної безпеки та безпечне використання додатків сучасного інформаційного сервісу та впровадження нових додатків

Ключові слова: випадкові дані, шумові процеси, захист інформації, перетворення, обробка, статистичне вирівнювання

UDC 621.391.25
DOI: 10.15587/1729-4061.2018.139755

ENHANCEMENT OF PRODUCTIVITY OF RANDOM SEQUENCES GENERATION FOR INFORMATION PROTECTION SYSTEMS

V. Bezshtanko
PhD, Head of Research Laboratory
Laboratory of Research Center*
V. Bondarenko
PhD, Deputy Chief
First Management of Department security information
State Service of Special Communications and Information Protection of Ukraine Solomyanska str., 13, Kyiv, Ukraine, 03110
O. Gavrylenko
PhD, Associate Professor
Department of IT-Security
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058
S. Yevseiev
Doctor of Technical Science, Senior Research
Department of Information Systems
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
E-mail: serhii.yevseiev@hneu.net
S. Ivanchenko
Doctor of Technical Science, Associate Professor
Department No. 1*
N. Kazakova
Doctor of Technical Sciences, Associate Professor, Head of Department
Department of computer, information and measurement technologies
Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020
R. Korolev
PhD, Senior Lecturer
Department of Combat Use and Operation of Automated Control Systems
Ivan Kozhedub Kharkiv University of Air Force
Sumska str., 77/79, Kharkiv, Ukraine, 61023
S. Mazor
PhD, Associate Professor
Department No. 3*
V. Romanenko
PhD, Head of Department
Department No. 4*
O. Fraze-Frazenko
PhD, Associate Professor
Department of computer, information and measurement technologies
Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020
*Institute of Special Communication and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Verhniokluchova str., 4, Kyiv, Ukraine, 03056

1. Introduction

At present, given the development of science and technology, there is a rapid growth of technical and technological possibilities for implementation of various information services and applications, required by the community. Modern information technologies ensure the implementation of tasks of varying difficulty with processing and transmitting large

data arrays, various calculations and decision making. Accordingly, they require the involvement of large computer resources, for which one of the main indicators is the operation rate of the applied information systems. The specified rate provides promptness and complexity of the implemented technologies.

One of the central issues of the safe use of modern information services and applications is guaranteeing information security, which requires the use of effective information protection systems. The needs for a rise in the performance of information technologies lead to relevant needs for performance of the information protection systems. In turn, these systems require high productivity of the generator equipment and random data sequences.

A particular issue, which also contributes to the need to enhance the productivity of generators, is the growth of potential possibilities for threats implementation and effective methods for statistical analysis. It is statistical analysis of random sequences that makes it possible to identify weaknesses that reduce their practical uncertainty.

There are many technologies and applications [1–10], which require the use of random data sequences. This is simulation, which provides an opportunity to study actual objects (processes) by replacing them with models [1]. These are cryptographic applications that provide information confidentiality thanks to the conversion with the use of the random key [2, 3]. It is data randomization for securing information from leaking through technical channels [4–6]. This is the digital generation of interferences to mask dangerous signals in the leakage channels [7–10], generation of passwords, protective codes, etc.

Thus, to use modern information services and applications safely and to ensure an effective information protection, random data sequences should be produced with an assigned quality and assigned rate – productivity, a requirement for which is constantly growing.

2. Literature review and problem statement

Currently, all methods and means for generation of random data sequences can be divided in two generations. One of them is an active generation. It includes traditional methods that have their implementations in the form of technical means. These methods are usually based on the conversion of some natural processes – physical sources that features of randomness in one degree or another. These methods are described in full detail in papers [11, 12].

An essential drawback of these methods and tools is a low generation rate or existence of statistical defects in sequences. The elimination of these defects requires the alignment of statistical characteristics, which, again, are realized at the expense of decreasing the rate. The methods of this generation are low-productive and incapable to sufficiently provide for the needs of modern protection systems.

The next generation includes the newest methods for generation of random data sequences, which differ from the existing ones by the fact that they are based on the quantum-mechanical theory. They use not conversion of natural random processes into a sequence, but the sequence itself is already a random process, formed from the spin states of elementary particles (electrons, protons, and neutrons). In accordance with the theorem of John Bell (1964), the generation by the specified method can at high rates ensure a complete uncertainty of the sequence. That is why numerous scientific papers deal with studying this issue.

Thus, paper [13] examined the possibilities of obtaining independent random binary data based on the quantum mechanical representation of natural processes (phenomena) that meet the criterion of non-fulfillment of the Bell inequality. In paper [14], in contrast to classical physics, which excludes existence of randomness in the full sense of the word, the Bell test was proposed, which according to the principle of the quantum theory makes it possible to obtain a random bit sequence. Article [15] substantiated the models of obtaining randomness from non-interacting and unreliable quantum devices. The proposed method for construction of the randomness extractor is protected from modern quantum attacks.

In paper [16], the possibility of intensifying a weak randomness with the use of quantum resources was shown. The randomness intensification protocol that includes the Bell experiment with sufficient non-fulfillment of its inequality was presented. Article [17] addressed quantum cryptography randomness, it proved the security of the new Protocol and substantiated the security against quantum attacks. In article [18], hardware implementation of the rapid random number generator with the photon integrated circuit and the electronic card of the programmable vent matrix was demonstrated.

However, all these quantum-mechanical generation methods have not undergone sufficient completeness in implementations yet. Despite the existence of certain samples of quantum technology, they still remain in the status of promising. This technique uses fundamentally innovative physical effects, where energy quanta – spins of elementary particles, rather that electricity, are used as data carriers. It currently bears an experimental rather that utility character and requires the appropriate development.

The methods of pseudo-generation, based of algorithmic complexity, can be separated in a particular class of obtaining random data sequences [2, 3]. A substantial merit of the latter is achievement of the desired generation rate, which is distinguished by the clock cycle frequency of an algorithm implementing tool. These methods are also the focus of a number of relevant papers. In particular, paper [19] examined the methods for construction of these generators, their theoretical and empirical properties with the required comparison. Article [20] deals with the use of random sequences generators for formation of cryptographic keys and, due to strict requirements for them, the possibility to replace these generators with pseudo-random generators. Paper [21] considered the possibilities of pseudo-random data implementation based on programmable logic integrated circuits, where fairly high generation rates were shown.

However, despite the proximity of statistical characteristics of pseudo-random to random data and possibilities to ensure the required generation rates, pseudo-randomness due to its algorithmic origin makes it possible to calculate and guess the sequence data. This is undesirable for information protection systems and limits the use of the pseudo-random generation methods it them.

Thus, the conducted analysis showed that the methods of sequence generation based on analog-to-digital conversion of noise processes remain relevant and demanded. Random data sequences for protection systems are necessary now and today. That is why they require improvement and effective application in practice. This is proved by the research of the

past years, published in the following papers. In paper [22], an experimental analysis of randomness during generating random sequences based on analog-to-digital conversion was carried out. Article [23] is dedicated to obtaining random sequences based on analog-to-digital conversion of the output of the semiconductor laser with the external resonator. In article [24], the description of model of random binary data source form physical sources was carried out. Paper [25] is devoted to the use of the properties of semiconductor lasers, which operate in a chaotic mode.

However, an increase in productivity in these works is carried out not due to the rational conversion of the noise process, but through the use of sources with range widening to the optical frequency range. Thus, it is a very effective approach to efficiency improvement, but there are other ways which also provide the opportunity to enhance efficiency both when using the classical methods of analog-to-digital conversion of noise processes with low Nyquist frequency [11, 12, 26], and with the use of laser devices, described in papers [23–25]. Theoretically, all continuous random processes have infinite count entropy. Although the actual physical sources of these processes are far from ideal, it is still possible to obtain high generation efficiency from them. Accordingly, the enhancement of generation productivity requires substantiation and the use of effective conversion methods.

As it has already been stated, the methods of generation of random sequences from physical sources do not always meet the needs for quality-rate indicators at present. As a rule, the right quality is ensured at low generation rates. Increasing the rate leads to a decrease in quality and appearance of statistical defects of a sequence. The causes of the stated above are:

– a mismatch of the parameters of the analog-to-digital conversion and the probability distribution density of a converted random process;

– a non-stationary random process used for analog-to-digital conversion.

Elimination of statistical shortcomings can be performed through the use of the methods of aligning statistical characteristics that increase the source entropy. The effective methods are:

– the method of von Neumann-Elias-Ryabko-Matchikina (sampling of equally probable combinations) [27–29];

– the method of Santha-Vazirani (code processing by linear code) [30, 31].

The specified methods make it possible to achieve high data randomness indicators. However, this is carried out at the expense of decreasing the generation rate, which is an essential drawback of these methods. An increase in rate is possible through the consolidation of the alphabet, which requires proper parameter optimization through alignment and harmonization with the analog-to-digital conversion stage.

Thus, the relevant scientific and technical problem is to ensure the productivity of existing methods and means of generation of random sequences from physical sources to meet the needs of modern information protection system.

In this case, the following tasks are unresolved:

1. Non-optimized factors and their parameters that affect enhancement of productivity of the analog-digital conversion of noise processes into random data sequences.

2. Efficiency was not harmonized and parameters of alignment of statistical characteristics of random sequences with the methods of analog-to-digital conversion were not optimized.

3. The tasks and the techniques for parameters adaptation to nonstationary converted processes at both stages of generation: analog-to-digital conversion and alignment of statistical characteristics were not substantiated.

3. The aim and objectives of the study

The purpose of this study is to improve productivity of the methods for random sequences generation based on optimization of analog-to-digital conversion of noise processes for provision of modern information protection systems.

To achieve the set aim, the following tasks were addresses in our research:

– to optimize the parameters of analog-to-digital conversion of noise processes that affect enhancement of productivity of random data sequences generation;

– to substantiate the selection of the method to ensure proper alignment of statistical characteristics of random sequences for information protection systems;

– to substantiate the ways of parameters adaptation at both stages of conversion as for non-stationary converted processes and changeability of other factors that affect the generation productivity.

4. Studying the factors and ways to enhance the productivity of random sequences generation

To explore the ways of enhancement of productivity of generation of random sequences from natural sources, it is convenient to represent the process of noise conversion in the form of two stages of conversion (Fig. 1):

1) the stage of the primary conversion of noise process $u(t)$ into data sequence X;

2) the stage of the secondary conversion of X into sequence Y with the view to eliminating statistical defects and aligning statistical characteristics.

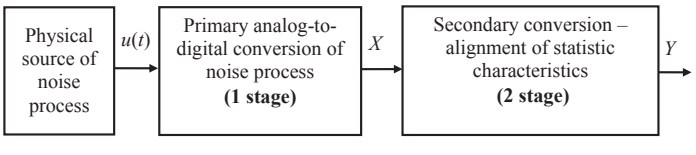

Fig. 1. Diagram of two-stage generation of random sequences from a physical source with analog-to-digital conversion and alignment of statistical characteristics

4. 1. The stage of primary conversion of the noise process. Substantiation of factors and their parameters

Let us have a physical source that forms noise process $u(t)$. A random signal $u(t)$ during conversion is discretized in time at the pitch Δt and quantized in the dynamic range with the pitch of Δu (Fig. 2).

Each random value $u=u(t_j)$ in time count with indices j=1, 2, 3,... is rounded up to the nearest quantum value of ui, multiple to Δu, $i=-N,..., -1, 0, 1,..., N$ (N is the natural number that determines the lower and upper limits of numbers of quantiles), so that $u_i=u(t_j)$. Each ui is matched against binary combination $X_k^n=(x_1, x_2, x_3, ..., x_n)$, lengths n, k=1, 2, 3, ... 2^n. Length n is selected with reasoning that $n \approx \log_2(2N)$ [32].

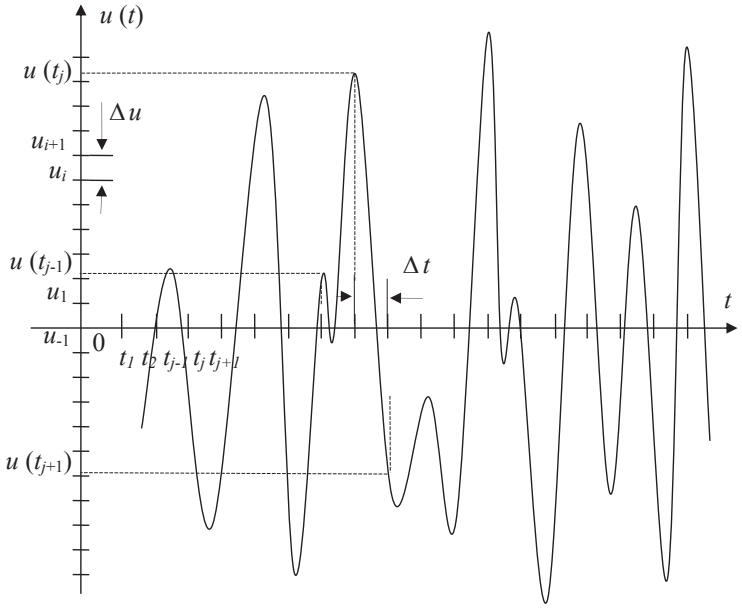

Fig. 2. Essence of the noise process conversion for random sequence generation

Thus, the main factors that affect the productivity of the analog-to-digital conversion of noise processes that are determined by the modern technical possibilities of implementation, for example, of spectral analysis are as follows:

1. The scale of quantization of the dynamic range of random process Δu_i, $i=-N, ..., -1, 0, 1, ..., N$, and the number of quantization levels $2N$.

2. Interval of random process discretization in time Δt, which depends on the frequency spectrum of a converted random process.

3. Non-stationarity and changeability of statistical properties of converted processes.

As it is well known from the theory of information [33], all random continuous processes that are designed for one count have infinitely large entropy:

$$H(U)=\lim_{\Delta u\to 0}\sum_i \omega(u_i)\Delta u\log_2\frac{1}{\omega(u_i)\Delta u}=$$
$$=\int_{-\infty}^{\infty}\omega(u)\log_2\frac{1}{\omega(u)}du+\lim_{\Delta u\to 0}\log_2\frac{1}{\Delta u}\sum_i\omega(u_i)\Delta u=$$
$$=h(u)+\lim_{\Delta u\to 0}\log_2\frac{1}{\Delta u}=\infty, \quad (1)$$

The simplest example of this conversion of the method for determining a random sign according to the level of noise in fixed points of time relative to the selection threshold – zero quantization zero [11]. If instantaneous noise intensity is less than zero ($u=u_{-1}<0$), logical zero ($x=0$) is formed at the output, if it is more than zero ($u=u_1>0$), unity is formed. In this case, one sign ($n=1$) is generated at one tact of discretization. This method is the result of advances of the last century, which corresponds to the level of technology development of those times, and low productivity of generation – the product of random sequence uncertainty and its generation rate. The rate of this generation is limited and depends on the Nyquist frequency of a converted process [26]. At an increase in the rate, various statistical defects of different nature, that required eliminating (statistical alignment), appeared in the generated data sequence, and those, in turn, led to a decrease in rate. Thus the generation effect was achieved due to rate economy at the alignment stage.

Another modern example of conversion of noise processes into random sequence is a known analog-to-digital conversion. It differs from the considered example by the expansion in the method of scale quantization conversion and the discretization interval. It enables the data sequence generation at higher rates and, accordingly, with higher productivity for the same random processes. As usual, to do this, one uses the standardized tools of the analog-to-digital conversion that mostly have a linear quantization scale or exponential or logarithmic scale that is proportional to some mathematical functions. If a noise process is stationary, it is relatively easy to select the quantization scale, which would ensure the required statistics of generated data.

Actual noise processes are far form stationary. Linear and other fixed quantization scales are not sufficiently adapted for distribution density. This causes the existence of statistical defects in the received sequences. These defects pose the need for applying effective methods of statistical alignment to these sequences.

where $h(u)$ is the differential entropy.

Although actual noise processes are far from ideal and entropy is not infinite, these processes still can provide an opportunity to obtain fairly high entropy, which would depend not only on the statistical properties of a random process, but also on the selected scale of non-zero Δu.

To ensure high productivity indicators, the task of generation of random data sequences requires the optimization of analog-to-digital conversion of random processes.

The optimization criterion for this conversion is maximum generation productivity:

$$H'(\%,Y)=\max[V_{\text{gen.}}H(\%,Y)], \quad (2)$$

where $V_{gen.}$ is the source generation rate:

$$V_{\text{gen.}}=\frac{\log_2(2N)}{\Delta t}. \quad (3)$$

Criterion (2) at both conversion stages can be ensured by performance of a rate maximum at a fixed generation quality, or a quality maximum at a fixed generation rate.

Thus, enhancement of productivity of generation of random data sequences is at the first stage reduced to obtaining the following solutions:

1. Substantiation of the optimum scale of quantization of dynamic range as for statistical properties of converted random process Δu_i.

2. Substantiation of the optimal interval of discretization of a random process over time Δt.

3. Adaptation of the quantization scale to non-stationarity of converted processes and changeability of other factors that affect productivity of the analog-to-digital conversion.

4. 2. The stage of secondary conversion of a sequence. Substantiation of effectiveness of the methods for alignment of statistical characteristics

At the second stage of generation of random data sequences, statistical characteristics are aligned. Proof effective meth-

ods for this alignment for information security systems include the method of sampling equally probable combinations (von Neumann-Elias-Ryabko-Matchikina) [27–29] code and the method of code processing (Santha-Vazirani) [30, 31].

The essence of the *method of sampling equally probably combinations* is as follows [27–29].

Sequence X is divided into the segments of the length n, which are certain combinations from the set of all possible X_k^n in the number of 2n. Conversion of X_k^n into the sections, from which resulting sequence Y is generated, is performed by the following rule (Table 1).

Table 1

Table of distribution of combinations X_k^n by the feature of equal weight *wt*

Weight of combination *wt*	Combinations $X_{k,wt}^n$ of weight wt	Number of combinations $X_{k,wt}^n$
$wt=0$	$X_{1,0}^n$	1
$wt=1$	$X_{2,1}^n, X_{3,1}^n, \ldots, X_{n,1}^n, X_{n+1,1}^n$	n
$wt=2$	$X_{n+2,2}^n, X_{n+3,2}^n, \ldots, X^n_{n+\frac{n(n-1)}{2},2}, X^n_{n+1+\frac{n(n-1)}{2},2}$	$\frac{n(n-1)}{2}$
.....		
wt	$X_{wt}^n\sum_{b=0}^{wt-1}C_n^b+1, X_{wt}^n\sum_{b=0}^{wt-1}C_n^b+1, \ldots, X_{wt}^n\sum_{b=0}^{wt}C_n^b-1, X_{wt}^n\sum_{b=0}^{wt}C_n^b$	$C_n^{wt}=\frac{n!}{wt!(n-wt)!}$
.....		
$wt=n-2$	$X_{n-2}^{n\,2^n-n-\frac{n(n-1)}{2}-1}, X_{n-2}^{n\,2^n-n-\frac{n(n-1)}{2}}, \ldots, X_{n-2}^{n\,2^n-n-3}, X_{n-2}^{n\,2^n-n-2}$	$\frac{n(n-1)}{2}$
$wt=n-1$	$X_{n-1}^{n\,2^n-n-1}, X_{n-1}^{n\,2^n-n}, \ldots, X_{n-1}^{n\,2^n-2}, X_{n-1}^{n\,2^n-1}$	n
$wt=n$	$X_n^{2^n}$	1

The set of all X_k^n is divided into subsets of combinations by the feature of equal weight wt, $wt=0\div n$. For each subset, we select combinations $X_{k,wt}^n$ so that the number should be multiple to certain $2^{k'}$, where k' is the natural number. Since division of combinations $X_{k,wt}^n$ by weight wt is subordinate to binomial law, k is selected from formula'

$$k'=k_{wt}=\left\lceil \log_2 C_n^{wt}\right\rceil. \quad (4)$$

The selected combinations is matched against the combinations of binary signs $Y_l^{k_{wt}'}$, $l=1, 2, 3,\ldots, 2^{k_{wt}'}$, from which original sequence Y is formed.

It is obvious that if sequence X is distributed according to the Bernoulli law, Y must be a perfectly random sequence with uniform distribution. In this case, it is relatively easy to calculate the rate of its conversion with the used of the Moivre-Laplace theorem, equating this rate to probabilities of appearance of equally probable combinations $X_{k,wt}^n$, to which original combinations $Y_l^{k'_{wt}}$ are assigned. For example, for $n=2$ the conversion rate will be derived from formula:

$$R=\frac{1}{\sqrt{2p(1-p)}}\phi\left(\frac{1-2p}{\sqrt{2p(1-p)}}\right), \quad (5)$$

where $\phi(x)=\frac{1}{\sqrt{2\pi}}e^{\frac{x^2}{2}}$ is the tabled Gaussian function; p is the probability of one of the binary signs of sequence X.

Actual sources have the distribution that is far from Bernoulli distribution, which is why it is not known what will be the effectiveness of this method for statistical alignment for actual sources. The conversion rate may also be different from the one determined from formula (5). That is why this method for actual sources requires particular research and experimentation. The specified drawbacks were eliminated in the methods for generation of random data sequence with code processing.

The essence of the method of code processing implies the following [30, 31].

Sequence X is divided into section of length n, the number of combinations of which is 2^n. X is converted into Y_l^m, $l=1, 2,\ldots, 2m$, from which resulting sequence Y is generated, by the following rule (Fig. 3).

The set of combinations X_k^n is divided into subsets of the same volume so that their number should be 2^m ($m<n$). Each subset is matched against certain Y_l^m from which original sequence Y is formed.

Obviously, combinations X_{lg}^n can be divided by subsets so that on average original Y would have a greater proximity to uniform distribution than X. In this case, conversion rate R is not a probabilistic magnitude both in the method as sampling equally probable combinations, and is strictly determined by parameters m and n. It is equal to:

$$R=\frac{m}{n}. \quad (6)$$

It should be noted that code processing can be implemented with the use of the linear noise immunity code and is reduced to a relatively simple operation of multiplication of X_k^n by check matrix, or by polynomial for a cyclic code [32]. The task for the search for effective codes by the maximum production criterion (2) with the assigned quality of the original sequence converges with the search for effective codes to ensure the maximum noise immunity [31]. In this case, it was shown that using linear codes for code processing, it is possible to achieve fairly high effectiveness, which is provided by the generation of large volumes of subsets $\left\{X_{l1}^n, X_{l2}^n, \ldots, X_{\text{lg}}^n, \ldots, X_{l2}^{n\,n-m}\right\}$, where $l=1, 2,\ldots, 2^m$.

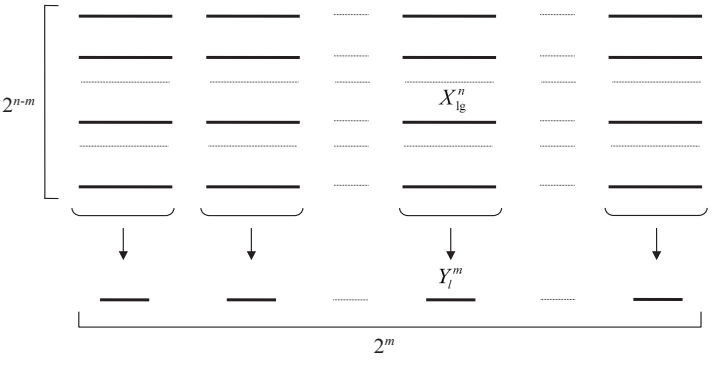

Fig. 3. Table of distribution of combinations X_k^n by subsets during conversion Y_l^m with code processing

Paper [31] gives the proof that such transformation ensures effectiveness of the alignment of statistical characteristics, not only for the Bernoulli probability distribution. Unlike the method of sampling equally probable combinations (von Neumann-Elias-Ryabko-Matchikina), the effectiveness of alignment using this method is ensued for a weakly random distribution, which takes into consideration statistical relationships among the data in a sequence [30].

Actual sources of random sequences are far from Bernoulli. Weak randomness also implies stationarity of the source, which not always has the place for actual sources.

Thus, an analysis of the methods for alignment of statistical characteristics of random data sequences was performed. They have the following effectiveness:

1. The method of sampling equally probable combinations (von Neumann-Elias-Ryabko-Matchikina) [27–29] is proof effective for the Bernoulli distribution of converted sequences. The conversion rate is asynchronous and depends on the statistical properties of a sequence.

2. The method of code processing (Santha-Vazirani) [30, 31] is proof effective not only for Bernoulli, but also for a weakly random distribution of converted sequences. The conversion rate is synchronous and is fully determined by constant parameters of the input and output combinations.

5. Results of studying the ways to enhance productivity of random sequences generation

5. 1. Substantiation of the optimum scale of quantization of dynamic range of random process

Actual noise processes are characterized by a fairly high degree of uncertainty, which is necessary to convert into random sequence with minimal losses in order to ensure the maximum count entropy during the process conversion.

For simplicity, let a random process, which is used for conversion into a random sequence, be stationary. Let us assume that there is an assigned ensemble of implementations of this random process, expressed by probability distribution density $\omega(u)$ with specified mathematical expectation a and root-mean-square deviation σ. To ensure maximum entropy

$$H(X)=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}p(X_k^n)\log_a\frac{1}{p(X_k^n)} \qquad (7)$$

it is necessary to satisfy the condition of the uniformity of sign combination X_k^n [26, 33, 34]. The specified equality is reduced to ensure the equality of areas under the curve of distribution density in Fig. 4, limited by the gradation of the dynamic range scale u.

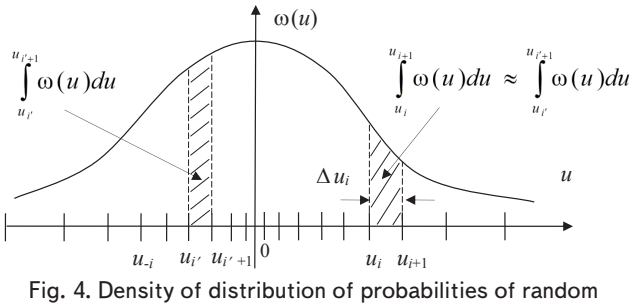

Fig. 4. Density of distribution of probabilities of random continuous magnitude u and the image of the example of scale, providing equality of probabilities during analog-to-digital conversion — areas between sections

If n is limited and $N=2^{n-1}$, it is possible to use the match of probabilities of combinations X_k^n and the fact that value $u\in[u_i; u_i+1[$:

$$p(X_k^n)=p_i(X^n)=@(u_i\le u<u_{i+1})=$$
$$=\int_{u_i}^{u_{i+1}}\omega(u)du=p(u_i). \qquad (8)$$

Quantization scale can be found based on meeting the condition of equality of integrals:

$$\int_0^{u_{\pm1}}\omega(u)du\approx\int_{u_{\pm1}}^{u_{\pm2}}\omega(u)du\approx\ldots\approx\int_{u_{\pm i}}^{u_{\pm(i+1)}}\omega(u)du\approx\ldots \qquad (9)$$

Thus, at the first stage of generation, optimization of the scale of quantization the dynamic range of a random process is reduced to ensuring the maximum possible magnitude N and satisfaction of condition (9).

1. A maximum of magnitude N ensures a maximum length n of code combination X_k^n, obtained from one count during analog-to-digital conversion.

2. Condition (9) ensures equality of probabilities $p(X_k^n)$ and, accordingly, the maximum entropy, calculated for one bit of random combination of X^n from ratio (7).

5. 2. Substantiation of the optimal interval of the random process discretization over time

An increase in the discretization interval of a continuous process leads to an increase in the rate of reading instantaneous values – counts. It is also known that a decrease in this interval for any random continuous process leads to a decrease in the difference between adjacent counts and an increase in statistical relations. That is why substantiation of the interval of discretization of a random process over time implies the substantiation of a certain minimum magnitude Δt_{min}, which would not lead to a decrease in generation productivity. This magnitude will be optimum by the criterion of a productivity maximum (2). In other words, it has to be such that counts of reading instantaneous values of the converted process still should not have the statistical dependence, or this dependence will not be significant with regard to the second stage of conversion. Obviously, ensuring the statistical independence of counts will make it possible to generate a sequence of statistically independent random data with rather high entropy.

Selection of interval Δt_{min} is influenced by two factors:

1. Schematic-technical limits to productivity of analog-to-digital converters.

2. Limitations of a converted process $u(t)$ by its spectral and statistical characteristics.

The first factor is associated with existence of the own capacity and inductivity in electronic element base, which in the modern circuitry are minimized by increasing the degree of micro scheme integration, using highly conductive materials, etc. Thus, today, examples of fast-acting tools are modern means of spectral analysis, such as the world-famous companies Rohde Schwarz of the type R&S®FSW85, R&S®FSWP50, R&S®FSMR50. They provide the possibility of measurement and analysis of continuous processes in the spectrum of up to 50÷85 GHz.

It should be noted that these are boundary frequencies of the electromagnetic field, accompanied by electrical currents. Application of the optical electronics in the range of

1012÷1015 Hz, where the carrier is not electric current, but a photon of light, will make it possible to increase essentially the indicated speed. These promising ways, explored in papers [12–17], ensure obtaining random sequences that belong to the new generation and are based on the quantum-mechanical theory.

The second factor which limits minimization of the reading interval is the Nyquist frequency of a random process and the statistical dependence of instantaneous values of counts [26]. It was already indicated that reading a process at the rate that exceeds the Nyquist frequency will lead to a decrease in the difference between instantaneous values of counts, and thereby to an increase in the statistic relations between them.

Thus, optimality of the interval of discretization of a random process over time Δt_{min} is not unambiguous. Its substantiation can be carried out from three points of view:

1. With provision of the maximum of uncertainty conversion at the stage of conversion of a continuous random process into a random data sequence at maximum rates without taking into consideration existence of possible statistical defects in a sequence. In this case, elimination of the latter is expected at the second stage of generation – the stage of alignment of statistical characteristics, which is performed at the expense of a decrease in the rate.

2. With provision of conversion of the maximum of continuous process uncertainty into the original sequence on condition that there is a minimum or no statistical defects in it altogether. An increase in reading rate should not lead to an increase or appearance of these defects. In this case, alignment of statistical characteristics of a sequence becomes unessential or unnecessary at all [35].

3. With provision of conversion of the maximum of continuous process uncertainty into the original sequence with the rate harmonization optimization at stages 1 and 2 of generation.

When it comes to the first point of view, the reading interval can be found using the theorem of Kotelnikov [26], which states that any analog signal that is finite by time and range can be fully represented in the form of $2\Delta F\Delta t$ counts, where ΔF is the signal spectrum width. In this case

$$\Delta t_{\min 1} = \frac{1}{2\Delta F} \tag{10}$$

as, for example, for n=8 and on condition of the optimal dynamic range scale (9). At the width of the spectrum of a converted noise process of 250 kHz, it is possible to obtain the random date sequence with the reading interval of 2 mks and productivity of about 128 Mbps.

From the second point of view, Δt_{min2} must be selected by empirical methods with the help of statistic testing a continuous process. It is expedient to carry out by means of accepting a certain basic value of the interval, for example, $\Delta t'_{min2}=\Delta t_{min1}$, and its gradual approximation to value $\Delta t_{min2}=\Delta t'_{min2}>\Delta t_{min1}$. In this case, the condition of statistical independence of counts must be met. Such interval ensures a low generation rate and has a lower boundary:

$$\Delta t_{\min 2} \geq \frac{1}{\Delta F}. \tag{11}$$

Thus, for the conditions of the previous example, the reading interval will increase and, accordingly, the generation rate will fall by more than 2 times, and so productivity will decrease and will not exceed 64 Mbps.

With respect to the third point of view, interval Δt_{min3} is derived so that in combination with the statistical alignment rate R, the criterion of random sequences generation should be met (2).

In this case, from all three points of view, reading intervals should be in ratio:

$$t_{min1}<\Delta t_{min3}<\Delta t_{min2}. \tag{12}$$

It should also be noted that the reading interval does not determine the final productivity of the source. To ensure the required quality, the sequence, resulting from the conversion of the physical noise process, is subject to alignment of statistical characteristics that will be associated with losses of rate indicators of the generation.

5. 3. Substantiation of selection of the effective method for the alignment of statistical characteristics for information security systems

One of the main challenges for any information security system is to guarantee safety, which in the part of using the generators of random data sequences requires the assigned statistical reliability from them. In turn, the necessary reliability can be provided only by proof effective methods.

Unlike the method of sampling equally probable combinations (von Neumann-Elias-Ryabko-Matchikina) [27–29], the method of code processing (Santha-Vazirani) [30, 31] provides proof effectiveness for a weakly random distribution. A weakly random distribution takes into consideration relationship of each bit of a random data sequence with its prehistory, which decreases the uncertainty degree and makes it possible to guess data with a certain degree of reliability. This is a significant factor for information protection systems, which should provide security of information resources.

Almost all practical sources have a weakly random distribution. That is why to align statistical characteristics, it is expedient to use the method of code processing (Santha-Vazirani) as proof effective. It is convenient to demonstrate the effectiveness of this method with the help of Fig. 5. It contains the specified diagrams of dependence of the entropy of the output sequence on the entropy of the input for the theoretical maximum and practical effectiveness of code processing, as well as in the absence of code processing.

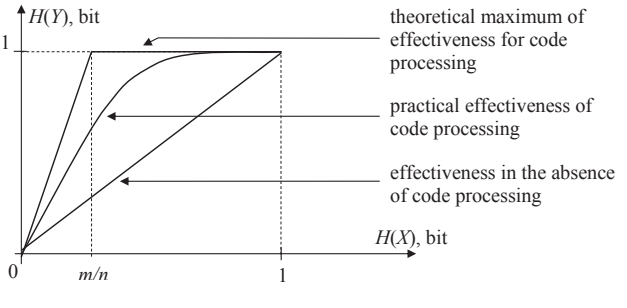

Fig. 5. Graphical image of dependence of entropy of the output sequence from the entropy of the input for theoretical maximum and practical effectiveness of code processing, as well in the absence of code processing

The method of code processing has a relatively small complexity of implementation. For example, the use of the

linear code makes it possible to implement code processing by simple operation of multiplication of section of an input sequence by the check code matrix or by a polynomial for a cyclic code. Improvement of the effect of alignment of statistical characteristics for the criterion of productivity maximum (2), is achieved through the code extension and using perfect codes during code processing [34].

5. 4. Substantiation of the ways of conversion parameters adaptation to non-stationarity of converted processes

Under condition of non-stationarity of a converted process and changeability of other factors that affect the productivity of the generation, the adaptation of parameters is necessary at all stages of conversion. Adaptation is needed during the operation of the generation tool, and therefore it is possible by application of feedback with the necessary adjustment of parameters, as shown in Fig. 6.

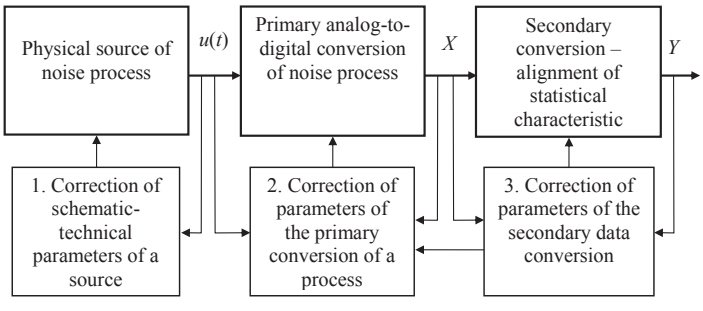

Fig. 6. Block-diagram of two-stage generation of random sequences from a nonstationary physical source with adaptation of parameters of analog-to-digital conversion and alignment of statistical characteristics

1. Adjustment of schematic-technical parameters of a source is carried out based on a statistical analysis of the generated noise process $u(t)$ by adaptation (intensification or weakening) of a signal to stationarity features. To do this, it is possible to use the Slutsky rule, which has the form:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T R(\tau)\mathrm{d}\tau = 0, \qquad (13)$$

where $R(\tau)$ is the function of noise process correlation:

$$R(\tau) = \frac{1}{T}\int_0^T u(t)u(t-\tau)\mathrm{d}\tau. \qquad (14)$$

2. Two tasks are solved during adjustment of parameters at the first stage of analog-to-digital conversion:

– based on statistical analysis of noise process $u(t)$, the scale of analog-to-digital conversion is generated and adapted to probabilities distribution density;

– based on statistic testing of sequence X, the number of quantization levels is adjusted, which will lead to consolidation or partitioning of the analog-to-digital conversion scale [36, 37].

3. Two tasks are solved during adjustment of parameters at the second stage of alignment of statistical characteristics of sequence X:

– the code for performing code processing is selected based on statistical testing of sequence X, which must provide the necessary quality of resulting sequence Y;

– based on statistic testing of sequence Y, the interval of discretization of the converted random process over time is adjusted and parameters of code processing are adapted up to providing the required quality of Y [36, 37].

6. Discussion of results of studying the ways to enhance the productivity of random sequences

Enhancement of productivity of generators of random sequences, caused by needs of modern information protection systems, requires a comprehensive solution at both stages of generation.

Thus, at the first stage of generation by the criterion of productivity maximum, we proposed:

– optimization of the quantization scale of the dynamic range of a converted random process;

– optimization of the interval of discretization of a random process over time.

Optimization of the quantization scale is reduced to ensuring a maximum possible magnitude of quantization levels N and meeting condition (8) – equalities of areas by the scale marks under the curve of the probability distribution density. An increase in N during conversion of noise process $u(t)$ leads to an increase in number of bits n ($n \approx \log 2(2N)$) of combinations of X_k^n, k=1, 2, 3,..., 2^n, and scale optimization to equal probability of these combinations for all k. Thus, at an increase in magnitude N by two times, for example, from 2,048 to 4,096, number of bits of the output combination n will increase from 10 to 11. In this case, generation rate and at maintaining equal probability X_k^n, productivity will also increase by 1.1 times.

Optimization of the interval of discretization of the random process over time Δt_{min} is not unambiguous. We used three points of view during its substantiation:

– provision of maximum of reading rate, at an increase of which productivity will not grow;

– provision of the maximum of reading rate, at which there are still no statistical relations between counts;

– provision of reading rate between the above specified maxima depending on the effectiveness of the alignment of statistical characteristics.

Obviously, at a decrease of interval of discretization over time due to appearance of statistical relationships between counts, entropy $H(X)$ will decrease. In other words, despite high productivity of the primary conversion, sequence X can be generated at high speed, but with insufficient quality. That is why it is necessary to enhance this quality, which is performed through the alignment of statistical characteristics.

At the second stage, in order to align statistical characteristics, it is proposed to use the method of code processing. Code makes it possible to enhance statistical quality of a sequence due to a certain proof effective conversion that is associated with a decrease in rate.

We performed evaluation of the effectiveness of code processing for some codes, specifically, the parity check codes, such as Hamming code, BCH code, and Golay code. Effectiveness is expressed by the conversion rate and dependence of entropies after code processing and before code processing. The evaluation results are shown in Table 2.

The values of Table 2 have the graphic representation in Fig. 7.

Table 2

Dependences of entropies after and before code processing with the use of parity check codes of Hamming, BCH, and Goley

Absence of code processing	Code processing with the use of codes					
	BCH (31,21)	Golay (24,12)	Parity verification (4,3)	Parity verification (11,10)	Hamming (15,11)	Hamming (63,57)
Rate of code processing: $R=m/n$						
1	0.32	0.5	0.25	0.09	0.27	0.095
$H(X)$, bits	Entropy $H(Y)$, bit					
0.011	0.035	0.023	0.037	0.081	0.042	0.116
0.045	0.140	0.091	0.140	0.287	0.164	0.410
0.081	0.248	0.162	0.230	0.460	0.283	0.633
0.141	0.426	0.283	0.372	0.680	0.462	0.858
0.194	0.567	0.387	0.499	0.805	0.594	0.948
0.242	0.678	0.480	0.589	0.881	0.694	0.982
0.286	0.765	0.562	0.662	0.927	0.771	0.994
0.327	0.832	0.635	0.722	0.956	0.829	0.998
0.365	0.882	0.700	0.770	0.973	0.874	0.999
0.402	0.919	0.755	0.812	0.985	0.907	≈1
0.436	0.946	0.803	0.847	0.991	0.933	
0.468	0.965	0.844	0.875	0.995	0.952	
0.610	0.997	0.961	0.958	0.999	0.999	
0.722	0.999	0.994	0.987	≈1	≈1	
0.811	≈1	0.999	0.991			
0.881		≈1	0.994			
0.971			0.999			

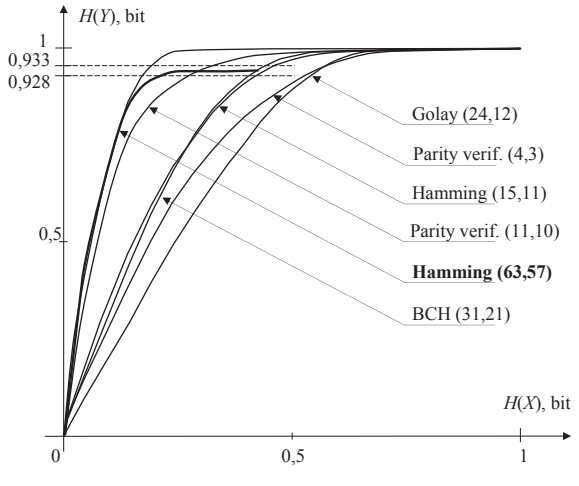

Fig. 7. Diagram of dependence of entropies after and before code processing with the use of parity check codes of Hamming, BCH and Goley

Similarly to the theoretical research, the experimental research into effectiveness of code processing using the Hamming code (63.57) as an example was carried out. Research into entropies was carried out using the Maurer test [36]. The obtained results are represented in Table 3 and in the form of the diagram in Fig. 7, which is highlighted with a line in bold.

As it can be seen from the diagram, the results of theoretical and practical research into code processing for the Hamming code (64, 57) almost coincide. The differences that occur in the upper region of the values $H(Y)$ are caused by test conditions. The values of entropies of 0.933 bits and 0.928 bits, represented on axis $H(Y)$, are the boundaries for positive testing that are determined by reliability degree. That is, if the result of testing gets within the specified boundaries, the studied sequence is considered to be sufficiently random, which corresponds to the theoretical 1 bit of entropy.

Table 3

Dependences of experimentally obtained entropies after and before code processing using the Hamming code as an example (63, 57)

$H(X)_{exp}$, bit	0.010	0.039	0.070	0.120	0.166	0.207	0.247	0.349	0.411
$H(Y)_{exp}$, bit	0.118	0.398	0.604	0.807	0.888	0.916	0.926	0.931	0.930

In the case of nonstationarity of a converted random process, enhancement of productivity requires the adaptation of conversion parameters at both stages of conversion. It should be done using feedback relationships as follows (Fig. 6):

– adjustment of circuit-technical parameters of a source (intensification, weakening of a signal) with the view to selecting the stationary noise component from the converted process;

– adjustment and adaptation of the quantization scale and the reading interval to residual non-stationarity of the source when converting the noise process at the first stage of generation;

– adjustment and adaptation of parameters of alignment of the statistical characteristics as for insufficiency of statistical quality and the sequence non-stationarity at the second phase of generation.

All kinds of adjustments at the stages of generation must be carried out based on statistical testing of output processes or data sequences [36, 37].

7. Conclusions

1. The optimization of factors that enable enhancement of productivity of generation of random date sequences from physical sources was proposed. Optimization of the factors was carried out using the two-stage representation of the generation: analog-to-digital conversion of noise processes and alignment of statistical characteristics of the resulting sequence. Such factors at the stage of analog-to-digital conversion are the scale of quantization of the dynamic range and the discretization interval of the converted random process over time. The condition, which must be met by the optimum scale and the boundaries for the optimal interval of discretization of the converted random process over time, was substantiated. Unlike the scale, the interval optimization is carried out by the criterion of maximum productivity not at the first stage of the analog-to-digital conversion, but taking into consideration the effectiveness of alignment of the statistical characteristics at the second stage of generation.

2. The use of the method of code processing (Santha-Vazirani), which is a proof effective method for weakly

random sources, was substantiated for alignment of statistical characteristics. When selecting the effective methods that increase the entropy of a random sequence, except for the specified method, we explored the method of sampling equally probable combinations (von Neumann-Elias-Ryabko-Matchikina). The method of code processing has a relatively simple implementation with the use of linear codes and is reduced to operation of multiplication of the section of input sequence by code check matrix, or by a polynomial of a cyclic code. However, the studies showed that this method is proof effective only for Bernoulli distribution of a data sequence. That is why it was turned down from the point of view of the requirements for information protection systems, for which the possibility of data guessing should be excluded. Enhancement of the effect of the alignment of statistical characteristics is achieved by code extension.

3. The methods for adaptation of generation parameters were proposed for productive obtaining random data sequences from non-stationary physical sources and taking into consideration the changeability of other factors that affect the productivity. They can be implemented based on the statistical control of outputs of generation elements and adjustment of the parameters of these elements through feedback relations.

The proposed optimization of parameters of random sequences generation and the ways of their adaptation to non-stationarity of a physical source in practice can provide a possibility to achieve high productivity indicators. They are relatively simple when it comes to implementation with the use of modern equipment and technologies in real time and can be effectively used in actual information protection systems.

References

1. Ivashchenko A. V., Sypchenko R. P. Osnovy modelirovaniya slozhnyh sistem na EVM. Leningrad: LVVIUS, 1988. 272 p.
2. Moldavyan N. A. Problematika i metody kriptografii. Sankt-Peterburg: Izdatel'stvo SPbGU, 1998. 212 p.
3. Muramatsu J., Miyake S. Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices // Mathematics for Industry. 2017. P. 177–198. doi: https://doi.org/10.1007/978-981-10-5065-7_10
4. Wyner A. D. The Wire-Tap Channel // Bell System Technical Journal. 1975. Vol. 54, Issue 8. P. 1355–1387. doi: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
5. Korzhik V. I., Yakovlev V. A. Neasimptoticheskie ocenki effektivnosti kodovogo zashumleniya odnogo kanala. Mosocw: Problemy peredachi informacii, 1981. P. 11–18.
6. Elliptic Curve Cryptography in Practice / Bos J. W., Halderman J. A., Heninger N., Moore J., Naehrig M., Wustrow E. // Lecture Notes in Computer Science. 2014. P. 157–175. doi: https://doi.org/10.1007/978-3-662-45472-5_11
7. Zhou H. Randomness and Noise in Information Systems. California Institute of Technology Pasadena, California, 2013. 436 p.
8. An experimental implementation of oblivious transfer in the noisy storage model / Erven C., Ng N., Gigov N., Laflamme R., Wehner S., Weihs G. // Nature Communications. 2014. Vol. 5, Issue 1. doi: https://doi.org/10.1038/ncomms4418
9. Implementation of two-party protocols in the noisy-storage model / Wehner S., Curty M., Schaffner C., Lo H.-K. // Physical Review A. 2010. Vol. 81, Issue 5. doi: https://doi.org/10.1103/physreva.81.052336
10. Unfair Noisy Channels and Oblivious Transfer / Damgård I., Fehr S., Morozov K., Salvail L. // Lecture Notes in Computer Science. 2004. P. 355–373. doi: https://doi.org/10.1007/978-3-540-24638-1_20
11. Bobnev M. P. Generirovanie sluchaynyh signalov. Moscow: Energiya, 1971. 240 p.
12. Metody i sredstva generacii sluchaynyh bitovyh posledovatel'nostey / Torba A. A., Bobkova A. A., Gorbenko Yu. I., Bobuh V. A.; I. D. Gorbenko (Ed.). Kharkiv: Izd-vo «Fort», 2012. 232 p.
13. Colbeck R., Renner R. Free randomness can be amplified // Nature Physics. 2012. Vol. 8, Issue 6. P. 450–453. doi: https://doi.org/10.1038/nphys2300
14. Full randomness from arbitrarily deterministic events / Gallego R., Masanes L., De La Torre G., Dhara C., Aolita L., Acín A. // Nature Communications. Vol. 4, Issue 1. doi: https://doi.org/10.1038/ncomms3654
15. Chung K.-M., Shi Y. Wu X. Physical randomness extractors: generating random numbers with minimal assumptions. URL: https://arxiv.org/pdf/1402.4797.pdf
16. Mironowicz P., Gallego R., Pawłowski M. Robust amplification of Santha-Vazirani sources with three devices // Physical Review A. 2015. Vol. 91, Issue 3. doi: https://doi.org/10.1103/physreva.91.032317
17. Robust device-independent randomness amplification with few devices / Brandao F. G. S. L., Ramanathan R., Grudka A., Horodecki K., Horodecki M., Horodecki P. et. al. // URL: https://arxiv.org/abs/1310.4544
18. Real-time fast physical random number generator with a photonic integrated circuit / Ugajin K., Terashima Y., Iwakawa K., Uchida A., Harayama T., Yoshimura K., Inubushi M. // Optics Express. 2017. Vol. 25, Issue 6. P. 6511. doi: https://doi.org/10.1364/oe.25.006511
19. Gurubilli P. R., Garg D. Random Number Generation and its Better Technique. Computer Science and Engineering Department, Thapar University, Patiala, 2010.
20. Elsherbeny M. N., Rahal M. Pseudo – Random Number Generator Using Deterministic Chaotic System // International Journal of Scientific & Technology Research. 2012. Vol. 1, Issue 9. P. 95–97.

21. Kozierski P., Lis M., Królikowski A. Parallel uniform random number generator in FPGA // Poznan University of Technology, Academic Journals: Computer Application in Electrical Engineering. 2014. Vol. 12. P. 399–406.
22. 54 Gbps real time quantum random number generator with simple implementation / Yang J., Liu J., Su Q., Li Z., Fan F., Xu B., Guo H. // Optics Express. 2016. Vol. 24, Issue 24. P. 27475. doi: https://doi.org/10.1364/oe.24.027475
23. Minimal-post-processing 320-Gbps true random bit generation using physical white chaos / Wang A., Wang L., Li P., Wang Y. // Optics Express. 2017. Vol. 25, Issue 4. P. 3153. doi: https://doi.org/10.1364/oe.25.003153
24. Chaotic laser based physical random bit streaming system with a computer application interface / Shinohara S., Arai K., Davis P., Sunada S., Harayama T. // Optics Express. 2017. Vol. 25, Issue 6. P. 6461. doi: https://doi.org/10.1364/oe.25.006461
25. Argyris A., Pikasis E., Syvridis D. Gb/s One-Time-Pad Data Encryption With Synchronized Chaos-Based True Random Bit Generators // Journal of Lightwave Technology. 2016. Vol. 34, Issue 22. P. 5325–5331. doi: https://doi.org/10.1109/jlt.2016.2615870
26. Baskakov S. I. Radiotekhnicheskie cepi i signaly. Moscow: Vysshaya shkola, 1988. 448 p.
27. von Neuman J. Various Techniques Used in Connection with Random Digits // Monte Carlo Method, Applied Mathematics. 1951. P. 36–38.
28. Elias P. The Efficient Construction of an Unbiased Random Sequence // The Annals of Mathematical Statistics. 1972. Vol. 43, Issue 3. P. 865–870. doi: https://doi.org/10.1214/aoms/1177692552
29. Ryabko B. Ya., Machikina E. P. Effektivnoe preobrazovanie sluchaynyh posledovatel'nostey v ravnoveroyatnye i nezavisimye // Problemy peredachi informacii. 1998. Vol. 35, Issue 2. P. 23–28.
30. Santha M., Vazirani U. V. Generating quasi-random sequences from semi-random sources // Journal of Computer and System Sciences. 1986. Vol. 33, Issue 1. P. 75–87. doi: https://doi.org/10.1109/sfcs.1984.715945
31. Ivanchenko S. O., Parshukov S. S. Obgruntuvannia metodu heneratsiyi vypadkovykh poslidovnostei z kodovoiu obrobkoiu dlia kryptohrafichnykh system zakhystu informatsiyi // Spetsialni telekomunikatsiyni systemy ta zakhyst informatsiyi: Tematychnyi vypusk "Matematychni metody prykladnoi kryptohrafiyi". 2007. Issue 1 (13). P. 152–155.
32. Ivanchenko S. O., Zaitsev O. D. Metod vysokoproduktyvnoho peretvorennia shumovykh syhnaliv u vypadkovu poslidovnist // Spetsialni telekomunikatsiyni systemy ta zakhyst informatsiyi. 2009. Issue 2 (16). P. 140–144.
33. Gallager R. G. Teoriya informacii i nadezhnaya svyaz'. Moscow: Sovetskoe radio, 1974. 720 p.
34. Mak-Vil'yams F. Dzh., Sloen N. Dzh. A. Teoriya kodov, ispravlyayushchih oshibki. Moscow: Svyaz', 1979. 744 p.
35. Murry H. F. A General Approach for Generating Natural Random Variables // IEEE Transactions on Computers. 1970. Vol. C-19, Issue 12. P. 1210–1213. doi: https://doi.org/10.1109/t-c.1970.222860
36. Maurer U. Provable Security in Cryptography // Diss. ETH No 9260. 1990. P. 86–93.
37. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Bassham L. E., Rukhin A. L., Soto J., Nechvatal J. R., Smid M. E., Barker E. B. et. al. National Institute of Standards and Technology, 2010. 131 p. doi: https://doi.org/10.6028/nist.sp.800-22r1a