Original scientific paper

Study of a New Method of Radio-Sensor Identification of Radio-Electronic Devices

Konstantin A. Boikov

***Abstract* — The purpose of this work is to increase the protection of radio-electronic devices from illegal cloning, by studying a new physically unclonable functions (PUF) connected with the own electromagnetic radiation of a radio-electronic device. The work uses experimental research methods to record the electrical component of the electromagnetic field emitted by the product - the signal radio profile (SRP). Correlation analysis methods for product authentication, Pearson's statistical agreement method for identification are used. The practical significance of the work lies in the possibility of using the SRP to identify a group of devices and radio-technical protection of a radio-electronic product from fakes and illegal copies.**

***Keywords* — identification, authentication, signal radio profile, Pearson's criterion, radio electronic unit, correlation analysis.**

I. Introduction

THE emergence of new high-tech solutions in the market of the radio-electronic industry for manufacturers of original radio-electronic products is often accompanied by serious intellectual and legal and economic losses. This is happening as a result of an increasing number of counterfeits - counterfeit products. Modern methods of protecting radio electronic devices (RED) from illegal cloning and reverse engineering - reengineering (hardware encryption, hashing, digital watermarking) help to solve this problem only partially, since the disadvantages of most of the listed protective measures are significant hardware costs and, as a result, high energy consumption [1]. This approach contradicts modern requirements of minimizing the area occupied by a device on an integrated circuit chip, speed and energy saving.

One of the alternative methods of RED authentication are PUFs, which are much more economical to implement than the above protection methods [2]. PUFs are based on the use of the technological spread of parameters of integrated circuits - the values of threshold and reference voltages, signal propagation delays, the frequency range of the operation of individual components. Parameter deviations (technological variability) inherent in any technological process and causing corresponding variations in the formed physical structures are relatively recently used to ensure the security of integrated circuits, to authenticate them, and to generate various kinds of cryptographic keys. These PUFs directly use some manufacturing features of the circuit.

PUF is a hardware analogue of the implementation of hash functions, with a difference in the output value based on the uniqueness of a particular integrated circuit (or component), and not on a mathematical algorithm. The argument at the PUF input is called a request (RQ), and the output value is called a response (RTV) [3]. Obviously, for some integrated circuit (or circuit component), the set of requests $\{RQ_0, ..., RQ_{N-1}\}$ will be uniquely displayed in the set of responses $\{RTV_0, ..., RTV_{N-1}\}$ using PUF.

The main safety problem of using PUF arises in the contract manufacturing of microcircuits (fabless) and lies in the potential unreliability of the manufacturer, usually located in another country. In particular, the use of PUF to protect against counterfeiting does not protect against illegal overproduction of products in excess of the ordered quantity (the so-called Night-Shift Problem). In addition, the use of PUF as part of the implementation of cryptographic algorithms leaves the possibility of reading request-response pairs by the manufacturer [4]. Along with this problem, the PUF also does not allow identification, that is, to establish the identity of an unknown RED to a known one based on the coincidence of parameters.

To solve these problems, this paper considers a new type of PUF - a complex SRP obtained by registering the electrical component of its own electromagnetic radiation of radio-electronic units of the RED. The request for such a PUF has a disturbing effect on the radio-electronic unit, and the response is a unique SRP.

II. Materials and Methods

The purpose of the presented study is to increase the protection of radio-electronic devices from illegal copying and reproduction, through the study of a new PUF acquired with a technological spread in the parameters of electronic components. This PUF is associated with the own electromagnetic radiation of a radio electronic device and reflects its individual characteristics. To achieve this goal, it is necessary to solve the problems of registering the SRP, decomposition and extraction of its main parameters, as well as authentication and identification of complex electronic components by statistical methods.

To conduct research on identification, experimental samples (ES) and measuring equipment are required. As an ES, the uniqueness and identity of which must be determined by their SRP, 20 radio-electronic units were produced. These RED consist of parallel-connected switches on a bipolar (BP) and MOSFET (Fig. 1).

Paper received October 06, 2022; revised June 14 2023; accepted June 22, 2023. Date of publication August 08, 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Vujo Drndarević.

Corresponding author Konstantin A. Boikov is with the MIREA – Russian Technological University, Russia (phone: 381-64-6100100; e-mail: nauchnyi@yandex.ru).

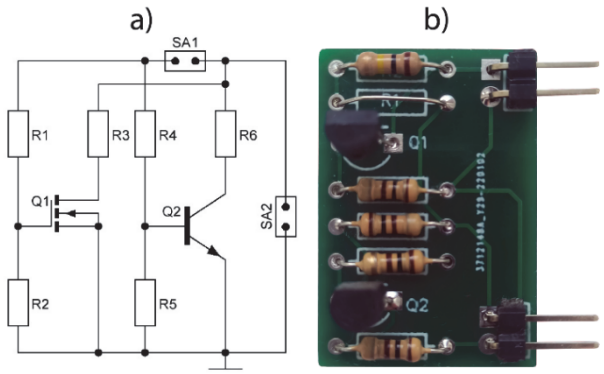

Fig. 1. Experimental sample – a composite radio-electronic unit: a) electrical circuit diagram, b) general view. *Source:* compiled by the author.

The +5 V control voltage is connected to the SA2 connector, supplied to the gate of the MOSFET Q1 and the base of the BP transistor Q2 by closing the SA1 contacts. R1 - jumper, R2 - pull-up resistor 100 kΩ, R3, R6 - load 100 Ω, R4, R5 - voltage divider.

The presence of filtering and parasitic capacitances in the ES when a control voltage is applied leads to a redistribution of energy between the filtering elements and parasitic reactive storage, which has an oscillatory character. The attenuation of oscillations here will depend on the ratio of the load parameters of consumers and storage devices, and the lower the load of the consumer, the slower the oscillations decay. In the presented electronic node, there is an occurrence of oscillatory redistribution of energy between storage devices, which are the capacitances of gate dielectrics of the MOS structure, barrier and diffusion capacitances of p-n junctions of the BP transistor. The method of solving differential equations in work [5] determines the type of emerging damped sinusoidal oscillations:

$$U_{CB}(t) = U_0 e^{-\delta t} \sin(\omega t + \varphi), \qquad (1)$$

where U_0 is the initial amplitude of oscillations (integration constant depending on the values of storage parameters), δ is the attenuation coefficient, ω is the angular frequency of oscillations, φ is the initial phase of oscillations (integration constant depending on the values of storage parameters).

Since an electronic node usually consists of a group of components, the final SRP of the node is a superposition of the SRP of the input and output circuits of its components, emitting free damped oscillations at times corresponding to the arrival of the control pulse [6]:

$$U(t) = \sum_{i=1}^{N} U_{CBi}(t) = \sum_{i=1}^{N} U_{0i} e^{-\delta_i (t - t_{0i})} \sin\left[\omega_i (t - t_{0i})\right], \qquad (2)$$

where t is the current moment of time, t_0 is the moment of the beginning of the radiation of the i-th oscillation.

Expression (2) is the basic equation for the SRP emitted by the electronic unit of the device and is valid only when the condition $t - t_{0i} \geq 0$ is met, and when $t - t_{0i} < 0$: $U_{CBi} = 0$. From a physical point of view, this means the absence of the i-th oscillation, at the moment when in the corresponding node or element there is no redistribution of energy between reactive storage devices. Also, in expression (2) there is no initial phase of radiation, since this parameter is indirectly included in t_0.

SRP radiation occurs when power is transferred from the power source to the radiating elements. In practice, direct emission from a source, such as supply lines or a single component, is most common. There are also emissions from connected power cables, data buses or signal lines. To register the emitted SRP, a measuring stand was built (Fig. (2).

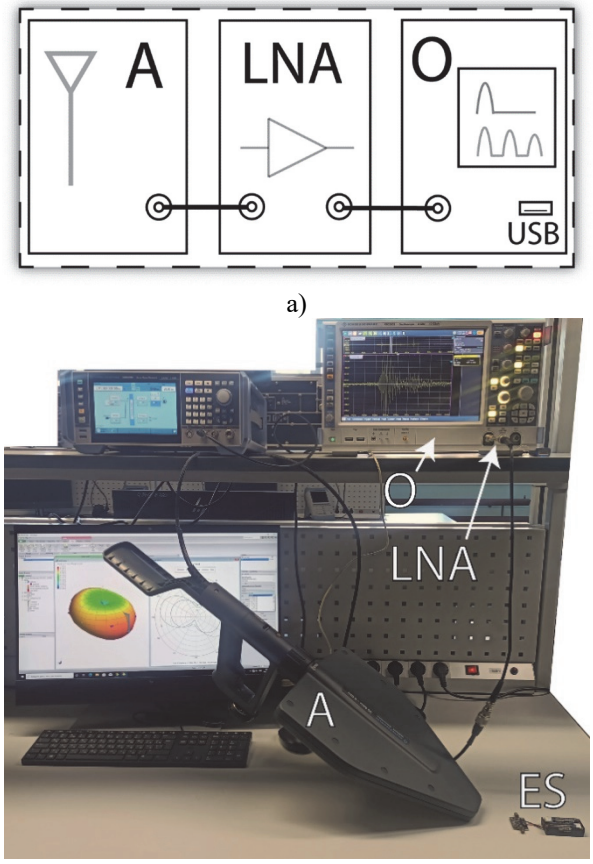

Fig. 2. Measuring stand: a) block diagram, b) photo *Source:* compiled by the author.

The SRP emitted by the ***ES*** is received by the broadband antenna ***A*** and amplified by the ***LNA***, a low-noise ultra-wideband amplifier. The amplified SRP is detected and recorded by an ultra-fast real-time oscilloscope ***O***. The data obtained as a result of the measurement is transferred to a personal computer for further processing. It is obvious that the detail of the study of the SRP depends on the bandwidth of the measuring system, the bit depth and sampling frequency of the oscilloscope. For registration of SRP with a duration of more than 5 ns, a frequency range of 0.1 - 3 GHz, sampling of 20 GSa/s is possible.

The study of the SRP is supposed to be carried out by the method of correlation analysis obtained from the studied object of the SRP, reflecting its radio engineering uniqueness, with the SRP of a similar RED (reference), by constructing a correlation function $r(h)$ [7]:

$$r(h) = \frac{\sum_{i=h}^{M+h} \left(Y_{1,i} - \overline{Y}_1\right) \cdot \left(Y_{2,i} - \overline{Y}_2\right)}{\sqrt{\sum_{i=h}^{M+h} \left(Y_{1,i} - \overline{Y}_1\right)^2 \cdot \sum_{i=h}^{M+h} \left(Y_{2,i} - \overline{Y}_2\right)^2}}, \qquad (3)$$

where M is the number of samples ("transformation window"), h is the number of the "window" position sample $(0 < h < K - M)$, K is the total number of SRP samples, $Y_1 = \frac{U}{U_M}$ is samples of SRP values a, $Y_2 = \frac{U_B}{U_{MB}}$ – is samples of SRP values b, $\overline{Y}_1 = \frac{1}{M}\sum_{i=h}^{M+h} Y_{1,i}$, $\overline{Y}_2 = \frac{1}{M}\sum_{i=h}^{M+h} Y_{2,i}$ is mean values of the samples, U is the value of SRP a at the sampling point, U_M is the maximum value of SRP a, U_B is the value of SRP b at the sampling point, U_{MB} is the maximum value of CRP b.

A detailed analysis to determine the identity of the SRP of the samples under study is supposed to be carried out by the decomposition method presented in work [8], with the extraction of parameters by means of a frequency-time transformation:

$$X(f,h) = \sum_{h=0}^{K-O}\left[\sum_{c=h}^{O-1+h} U(O)\exp\left(-j\frac{2\pi fc}{O}\right)\right], \quad (4)$$

where $X(f, h)$ is the discrete time-frequency spectrum of the signal, $U(O)$ is the signal sampled in time, o is the sample number, f is the frequency, O is the number of points that form the "window" of the transformation.

III. Results

As a result of the tests, 20 SRP were obtained, one from each experimental sample. The SRP of ES No. 1 was taken as the benchmark. The type of the benchmark and its correlation analysis with the SRP of a randomly selected EO No. 12 is shown in Fig. 3.

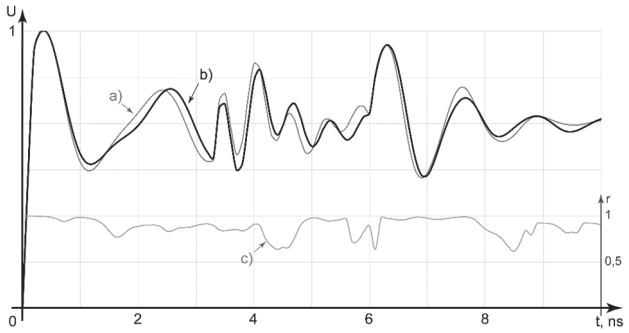

Fig. 3. SRP: a) benchmark, b) sample No. 12, c) correlation function. *Source:* compiled by the author.

As can be seen from this figure, the correlation function on the time axis falls below 0.9, reaching 0.6, which on the Chaddock scale [9] means a noticeable correlation (the curves are similar). Thus, a certain identity between the SRP is still traceable.

In a similar way, a correlation analysis of the SRP was carried out for each of the presented samples. For a detailed study of the identity of the SRP (that is, identification), the decomposition of the SRP was carried out and the main parameters of the SRP were obtained from the frequency-time spectrum (Fig. 4).

As can be seen from Fig. 4, the SRP consists of four emitters (N = 4). After the decomposition operation (in work [8] the operation of decomposition and extraction of parameters is described in detail), it is possible to obtain a table of parameters of these emitters.

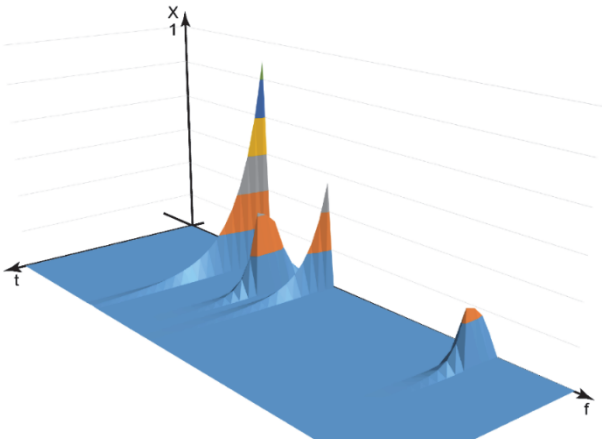

Fig. 4. Time-frequency spectrum of the SRP *Source:* compiled by the author.

TABLE 1. PARAMETERS OF THE EMITTERS OF THE BENCHMARK

Emitters	***f* [GHz]**	**δ [ns^{-1}]**	**t_0 [ns]**	**U_0**
***i*=1**	0.68	-0.31	0	0.84
***i*=2**	0.98	-0.43	0	0.4
***i*=3**	0.86	-0.75	5.3	0.96
***i*=4**	1.8	-0.85	3.1	0.73

Source: compiled by the author

Extraction of the parameters presented in expression (2) during decomposition makes it possible to find the number of elementary emitters N involved in the creation of the SRP. If N of the received SRP is less than the number of emitters of the reference N_P, then it should be concluded that some components of the node of interest are out of order, or that the measurement is incorrect. A set of SRP parameters will help to make a decision in this situation. In the case of equality, all elements of the node participate in radiation. If the number of emitters in the test SRP exceeds that of the benchmark, we can talk about incorrect calculation of this parameter, or incorrect measurement. Only in the case of equality of the number of emitters of the reference and the investigated SRP can we talk about further identification.

When making a decision on identification, it is possible to use Pearson's goodness-of-fit test, which is used to test the hypothesis that the empirical distribution corresponds to the expected theoretical distribution [10]:

$$\chi^2 = \sum_{j=1}^{k}\frac{\left(u_j - e_j\right)^2}{e_j} \quad (5)$$

where u_j is the observed frequency of the trait in the j-th group, e_j is the theoretical frequency of the trait in the j-th group.

This criterion can be used for any kind of functions, even with unknown parameters, which is a common case in analyzing test results. For applying Pearson's goodness of fit, it`s necessary to build a correspondence table of parameters received as a result of the SRP decomposition.

TABLE 2. PARAMETER CORRESPONDENCE TABLE

Emitters / ***Parameters***	***i*=1**	***i*=2**	***i*=3**	***i*=4**	u_j	e_j
f	1	1	1	1	4	4
δ	1	0	1	1	3	4
t_0	1	1	1	1	4	4
U_0	1	1	0	1	3	4

Source: compiled by the author

Table 2 shows four emitters ($N = 4$), and the result of the parameters of these emitters falling into the confidence interval (1 - the parameter fell into the confidence interval, 0 - the parameter did not fall into the confidence interval). The confidence interval itself was obtained as a result of numerous field tests and is nothing more than a technological spread of parameters. The confidence interval can also be determined from simulation results, or as a result of calculations using known reference data. The value u_j is the sum of the actual hits of the emitter parameters in the confidence interval, e_j is the sum of the expected hits of the emitter parameters in the confidence interval (for $N = 4$, $e_j = 4$).

Using expression (5) together with table 2, the coefficient χ^2 is calculated. For the case shown in Fig. 3, $\chi^2 \approx 0.97$. The results of empirical studies show that χ^2 is the probability of the identity of the studied SRP and the benchmark. Thus, the SRP presented in Fig. 3 are identical with a probability of 97% (RED belong to the same group with this probability). The analysis showed that all the studied samples were identified and identical to the benchmark with a probability of at least 95% ($\chi^2 \geq 0.95$).

It should be noted that during the experiment, the SRP of sample No. 1 was also taken for analysis (Fig. 5).

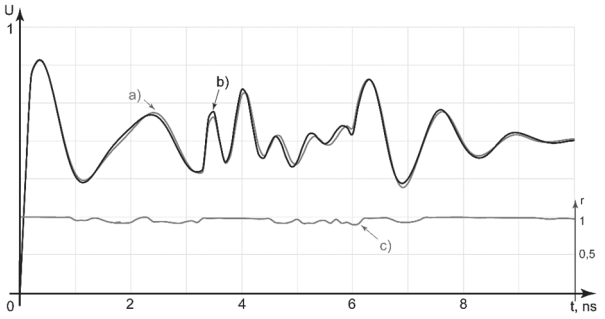

Fig. 5. SRP: a) benchmark, b) sample No. 1, c) correlation function. *Source:* compiled by the author.

As can be seen from this figure, the correlation function does not fall below 0.9, which, according to the Chaddock scale, means a very high correlation (the curves are identical). Thus, we can talk about the authentication of the sample under study, that is, the sample under study is the reference.

Multiple measurements show that the dependence of the reliability of SRP recognition on the values of the correlation function has the form shown in Fig. 6.

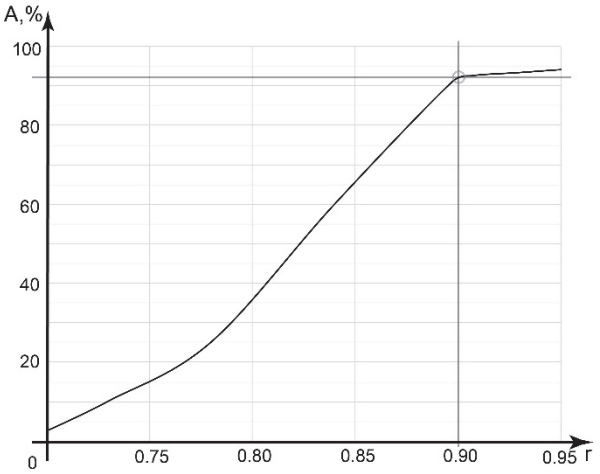

Fig. 6. Dependence of the reliability of recognition of SRP on the values of the correlation function. *Source:* compiled by the author.

IV. DISCUSSION

The data obtained during the experiment are similar to the data obtained as a result of modeling [11, 12], which indicates a high reproducibility of the radio sensor identification method. Correlation analysis in the study of the SRP allows you to authenticate the RED, that is, to determine its authenticity. In this case, the SRP is a unique PUF of a radio-electronic device. Authentication is not possible if the correlation function on the SRP time axis falls below 0.9. In this case, when constructing the parameter correspondence table and using Pearson's coefficient of agreement, it is possible to identify the RED with the probability of interest to the researcher. However, critically discussing the results obtained, the author does not recommend identifying the device at $\chi^2 < 0.95$, but the choice always remains with the researcher.

Based on the results of the research, it is possible to give a methodology for identifying the RED by the radio sensor method (Fig. 6)

The data obtained during the experiment are similar to the data obtained as a result of modeling (), which indicates a high reproducibility of the radio sensor identification method. Correlation analysis in the study of the SRP allows you to authenticate the RED, that is, to determine its authenticity. In this case, the SRP is a unique PUF of a radio-electronic device. Authentication is not possible if the correlation function on the SRP time axis falls below 0.9. In this case, when constructing the parameter correspondence table and using Pearson's coefficient of agreement, it is possible to identify the RED with the probability of interest to the researcher. However, critically discussing the results obtained, the author does not recommend identifying the device at $\chi_2 < 0.95$, but the choice always remains with the researcher.

Based on the results of the research, it is possible to give a methodology for identifying the RED by the radio sensor method (Fig. 7).

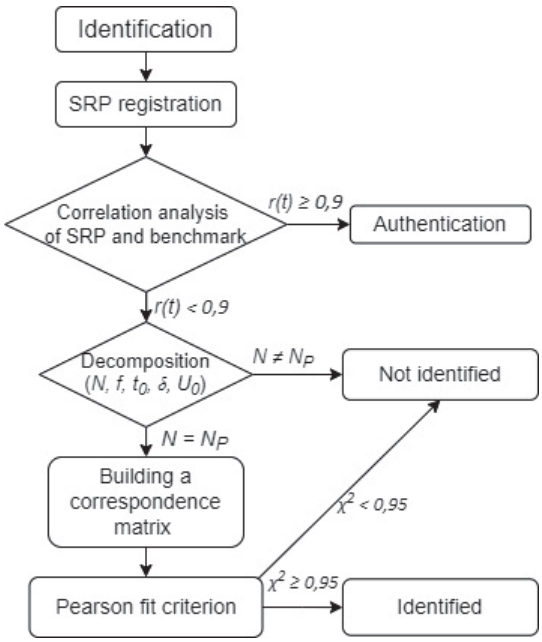

Fig. 7. Methodology for the identification of RED by radiosensor method. *Source:* compiled by the author.

As can be seen from the presented figure, identification and authentication are possible only if the number of emitters of the studied device and the benchmark are equal. Otherwise, the limits of applicability of the method end, since the initial data are erroneous, or the device under study is not in a functional state.

V. Conclusion

The paper presents the PUF based on the SRP obtained by recording the electric component of the near field of the electromagnetic radiation of the RED. This PUF was acquired by the product during the production process, due to technological tolerances for the parameters of the components. Restoration and analysis of such SRP by cross-correlation with the reference point, in combination with Pearson's goodness-of-fit criterion for decomposition and extraction of parameters, allows not only authentication, but also identification of the RED, which cannot be done by any of the known PUF today. The practical applicability of this method lies in the ability to distinguish the original radio-electronic product from the counterfeit remotely, without interfering with the operation of the device. The radio sensor identification technology itself allows using software-defined radio systems (SDR) for analysis, which should significantly speed up the recognition process, opening up further prospects for the development of the PUF direction, protection, authentication and identification of radio electronic devices in general.

REFERENCES

[1] V.N. Fedorets, E.N. Belov and S.V. Balybin, "Technologies for protecting microcircuits from reverse engineering in the context of information security," Moscow Russia: Technosphere, 2019.

[2] C. Herder, M.-D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[3] J. S. Kim, M. Patel, H. Hassan and O. Mutlu, "The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices," *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, Vienna, Austria, 2018, pp. 194-207, doi: 10.1109/HPCA.2018.00026.

[4] A. V. Semenov and A. V. Kostyuk, "Protecting the keys of microcircuits on physically unclonable functions in conditions of distrust of the silicon factory," *Information security issues*, vol. 2, pp. 63-68, 2015.

[5] K. A. Boikov, "Modeling and analysis of oscillatory redistribution of energy at own electromagnetic radiations in key radio-electronic circuits on MOSFETs," *Journal of radio electronics*, vol. 6, 2021, https://doi.org/10.30898/1684-1719.2021.6.14.

[6] K. A. Boikov, "Circuitry and electrodynamic modeling of the oscillatory process of energy redistribution in a bipolar transistor," *Izvestiya SFU, Technical sciences*, vol. 7, pp. 19-31, 2021.

[7] T. K. Thanh and T. T. Vinh, "The application of correlation function in forecasting stochastic processes," *Herald of Advanced Information Technology*, vol. 2(4), pp. 268-277, 2019, https://doi.org/10.15276/hait04.2019.3.

[8] K. A. Boikov, "Decomposition of the signal radio profile in passive radio sensor technical diagnostics and authentication of electronic devices," *Bulletin of the Voronezh State Technical University*, vol. 18, pp. 129-134*,* 2022.

[9] P. K. Shkodun, "Development of a set of diagnostic parameters for assessing the technical condition of rolling stock traction electric motors," *Izvestiya Transsib*, vol. 4 (44), pp. 56-65, 2020.

[10] R. Huang and H. Cui, "Consistency of chi-squared test with varying number of classes," *Journal of Systems Science and Complexity*, vol. 28(2), pp. 439-450, 2015, https://doi.org/10.1007/s11424-015-3051-2.

[11] K.A. Boikov, "Determination of the parameters of electronic devices by the method of passive radiosensor technical diagnostics," *News of higher educational institutions of Russia*, *Radioelectronics*, vol. 24(6), pp. 63-70, 2021. https://doi.org/10.32603/1993-8985-2021-24-6-63-70.

[12] Y. Su, J. Holleman and B. Otis, "A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations," *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, San Francisco, CA, USA, 2007, pp. 406-611, doi: 10.1109/ISSCC.2007.373466.