Svitlana CHAPLINSKA[1], Dmytro KOSTYRKO[2]

Opiekun naukowy: Elena NYEMKOVA[3]

SYSTEM UWIERZYTELNIANIA URZĄDZEŃ IOT ZA POMOCĄ WEWNĘTRZNEGO SZUMU ELEKTRYCZNEGO

Streszczenie: Zaproponowano system uwierzytelniania oparty na wewnętrznym szumie elektrycznym urządzeń elektronicznych. System działa w czasie rzeczywistym. System może być również wykorzystywany do ciągłej inwentaryzacji urządzeń IoT systemów cyberfizycznych. Przedstawiono wyniki badań eksperymentalnych w celu określenia właściwości uwierzytelniania urządzeń elektronicznych.

Słowa kluczowe: cyberbezpieczeństwo, Internet Rzeczy (IoT), system uwierzytelniania, wewnętrzny szum elektryczny

THE AUTHENTICATION SYSTEM OF THE IOT DEVICES BY INTERNAL ELECTRICAL NOISE

Summary: The authentication system based on internal electrical noise of electronic devises is proposed. The system operates in real time. The system also can be used for continuous inventory of IoT devices of cyber-physical systems. The results of experimental studies to determine the authentication characteristics of electronic devices are presented.

Keywords: cybersecurity, IoT, authentication system, internal electrical noise

1. Introduction

The commercialization of Internet of Things, SCADA and similar technologies has led to a dramatic decrease in information security of cyber-physical systems. The info-communication network, in addition to the usual personal computers, must be entered tens of billions of electronic devices (endpoints) such as Raspberry, physical encoders, routers, digital webcams, smart watches, fitness trackers and more, but the security of information sharing with these elements is very low, in some cases no protection from

[1] Lviv Polytechnic National University, student of department of Information Technology Security, specialty: cybersecurity, ch.svieta@gmail.com
[2] Ukrainian Academy of Printing, PhD student of department of Financial and Economic Security, Accounting and Taxation, specialty: management, kostyrkodm@gmail.com
[3] PhD, associate professor, Lviv Polytechnic National University, department of Information Technology Security, cyberlbi12@gmail.com

penetration into the system at those endpoint levels [1]. Low security leads to cyberattacks, where targets can be either specific cyber-physical systems or remote servers that are not connected to specific systems but connected to them through telecommunications [2]. Authentication with logical device names does not solve the problem of guaranteeing the information security; logical names can be replaced by a variety of attacks. Authentication for the use of cryptographic data presents one-factor procedures using data of the security of information systems required for multi-factor authentication.

Modern networks and computer systems are exposed to thousands of different attacks every day. The badge part of the attack is related to the violation of access rights when the attacker acts under the name of a legitimate user. This is possible due to poor authentication of the real user, usually one-factor. According to HP research, 70 percent of IoT devices have vulnerabilities [3]. For multi-factor authentication of individuals biometric methods were developed as a second factor. Electronic devices also need to develop similar methods, which will uniquely identify a specific device in critical object management systems, the Internet of Things, telemedicine and more.

2. Problem definition

Any electronic device consists of many components, which differ in parameters within the set of values. It is impossible to make exactly the same accessories at the micro level, so these differences are found in the deviations of the parameters at the macro level devices: the linear characteristics of the transmission paths, resonant frequencies, the ratio of noise at the input and output, and so on.

While operating electronic devices because of fluctuations of internal electromagnetic fields uncontrolled guidance occurs. Guidance can be propagated through coaxial lines, wires, or radiation in the form of electromagnetic waves. As a result, spurious signals appear, which are undesirable for the device to function properly. There are many causes for spurious signals. The main reason is a sudden change in current or voltage. In an electronic device connected to a power source, arises a complex picture of electromagnetic field interference; caused by the interaction of the components of the device. As a result, spurious signals appear in the output circuit of the electronic device. When designing devices, developers try to minimize these spurious signals, but it can't be reduced to zero.

Parameters of spurious signals (for example: phase, amplitude, frequency, dynamic spectrum) are determined by these internal electromagnetic fields, which depend on the elemental and structural features of the device. The complete identity of the devices cannot be ensured by the natural variation of parameters at the micro level, even with the same selection of components and their internal location. The output signals will be different for different devices of the same type, in other words, spurious signals on the output is individually similar to the individual biometrics of different people. Therefore, you can try to use them to identify electronic devices.

Spurious signals due to their minimization they are very small, most often they are the noise output of the device. The variety of electronic devices and, accordingly, the specificity of their recognition cause a considerable number of tasks that arise in the development of methods of authentication by electrical noise.

The scientific problems of authentication of electronic devices are devoted the theoretical and practical works of such scientists: O. V. Rybalsky, V. I. Solovyov,

V. V. Zhuravel, (problems of digital forensics) [4]; J. Hasse, T. Gloe, M. Beck (Geolocation of GSM Mobile Devices) [5]; J. Svoboda, M. Schanfein (encoder authentication on the local network) [6]; C. Yang, A. Sample (identification of electronic devices by electromagnetic radiation) [7], G.E. Suh, S. Devadas (authentication for physically non-cloned functions) [8] and others.

Although many scientific and practical studies have been conducted on the authentication of electronic devices by internal electrical noise [9], nevertheless a scientific problem of automatic dynamic authentication of electronic devices in real time by internal electrical noise remains relevant. Solving of this problem will increase information security of IoT.

The purpose of the work is to develop the structure of automatic dynamic systems of authentication IoT devices on the network. The following tasks are solved for this purpose:

1. the method of calculation of the template of authentication on an internal electric noise is offered;
2. the modular structure of the authentication system is proposed;
3. algorithms of work of modules of authentication system are offered.

3. Authentication by internal electrical noise

3.1. Model of authentication template

For stationary conditions the electronic device noise authentication template is calculated from the sequence of values of the normalized autocorrelation function for N noise counts x_n obtained by noise digitization:

$$AC_k(x,x) = \frac{1}{var(x)(N+1)} \sum_{n=1}^{N} (x_{k+n} - mean(x))(x_n - mean(x)) \quad (1)$$

where $var(x)$ – dispersion of the series x_n, $mean(x)$ – the average of the series x_n.

The B^I authentication template of electronic device I is a binary code, each value of which is characterized by an increase or decrease in the value of the autocorrelation function for two consecutive lag values [10]. The discrete values of the autocorrelation function must be converted to a sequence of zeros and ones by the rule:

$$B_k^I = \begin{cases} 1, AC_{k+1} \geq AC_k \\ 0, AC_{k+1} < AC_k \end{cases} \quad (2)$$

Comparison of two bit templates is made by Hamming's specific distance. The Hamming distance is normalized by the length M of the bit template:

$$H(B^I, B^J) = \frac{1}{M-1} \sum_{k=1}^{M} \left| B_k^I - B_k^J \right| \quad (3)$$

Indexes I and J belong to the bit templates, obtained from noise record I and J files. The length M of the autocorrelation function from which the bit template is calculated, is selected from the requirements of the needed recognition accuracy of a separate electronic device.

3.2. Experimental results

Audit of uniqueness of the form of autocorrelation function for each electronic device was carried out on the example of personal computers. Internal electrical noise was

digitized using a 16-bit analog-to-digital converter of the sound card and recorded to a file. The noise level was 150 μV. The recording length was 10 seconds at 44.1 kHz digitization rate. Starting with a recording time of 0.5 s the small-scale shape of the correlograms of the noise records did not change.

Experiments have shown:

4. firstly, the uniqueness of the shape of the noise signal correlogram of each electronic device, which is explained by the specific guidance noise caused by the operation of individual units of the device, the variation of the parameters of the component base of the devices at the microscopic level, as well as the design features of each of them;
5. secondly, the noise signal correlogram for each electronic device has a virtually unchanged, small-scale form for different recording files.

It has been proven experimentally that for one computer, the shape of the noise recording correlogram remains virtually unchanged for different noise recording files, figure1.

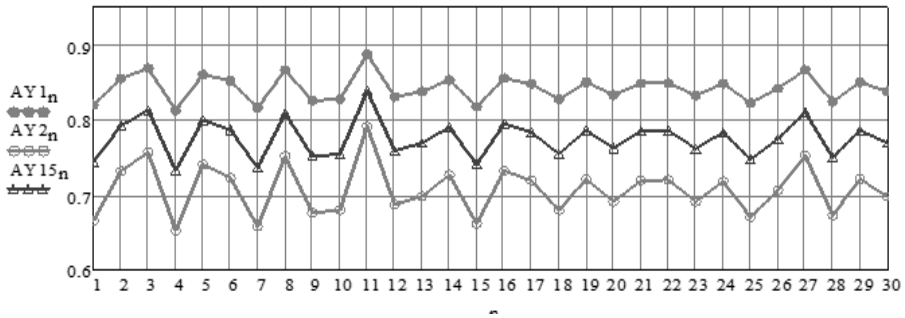

Figure 1. Fragments of correlograms of noise records made in different moments of time from one desktop computer

This form can be considered permanent for records made within one year. In the future, it changed slightly over time.

For different computers, the shape of correlograms of noise records differ from each other, figure 2.

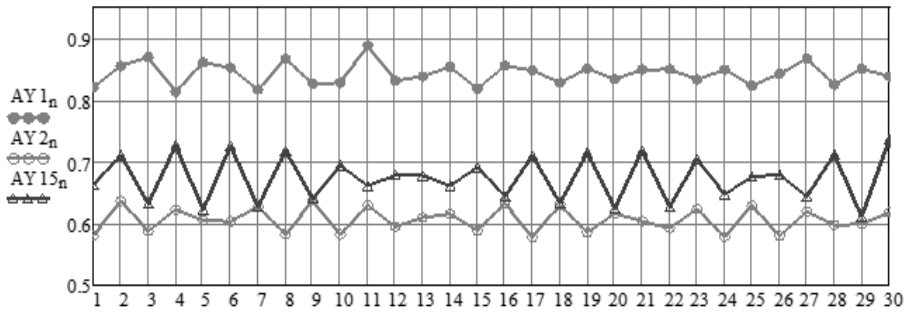

Figure 2. Fragments of correlogram of noise records made in different moments of time from three different desktops

Comparing the Hamming normalized distance for bit patterns calculated from the autocorrelation noise signals recorded from two computers and from one computer,

showed that the length of the template is 1000 bits for the authentication of the computers. The results of the dependence of the normalized distances between the templates of two PCs are shown in the table 1.

Table 1. The normalized Hamming distance depending on the length of the pattern

Length of the pattern	Normalized Hamming distance	
	Two different computers	One computer
10	0.000	0.000
50	0.060	0.000
100	0.070	0.000
150	0.087	0.013
200	0.095	0.010
300	0.100	0.010
400	0.103	0.010
500	0.098	0.008
600	0.095	0.007
700	0.099	0.009
800	0.101	0.009
900	0.102	0.009
1000	0.100	0.009

Further increase in bit template length does not increase the accuracy of normalized distance, which indicates that there is characteristic template length that almost completely characterizes a particular computer.

Studies on the stability of the bit template of noise have shown that the template may be distorted by external electromagnetic interference, such as from airport radars, radiation in the area of a TV-tower, pre-storm weather, as well as interference, which is distributed by the power network.

Such interferences are short-lived and their impact can be counterbalanced by the use of a form factor that allows the rejection of files with interference.

4. System of authentication

4.1. System's modules

Automatic authentication system for electronic devices "Noise-ID" is designed to perform dynamic authentication on a server in real time of electronic devices by internal electrical noise.
The hardware of the authentication system is shown in figure 3. The hardware is electronic devices connected to a local area network and a server.

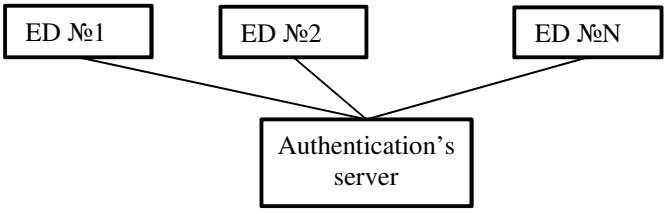

Figure 3. Hardware part of an authentication system

The software part of the authentication system is shown in figure 4. For each electronic device the algorithm of work of the software part is the same.

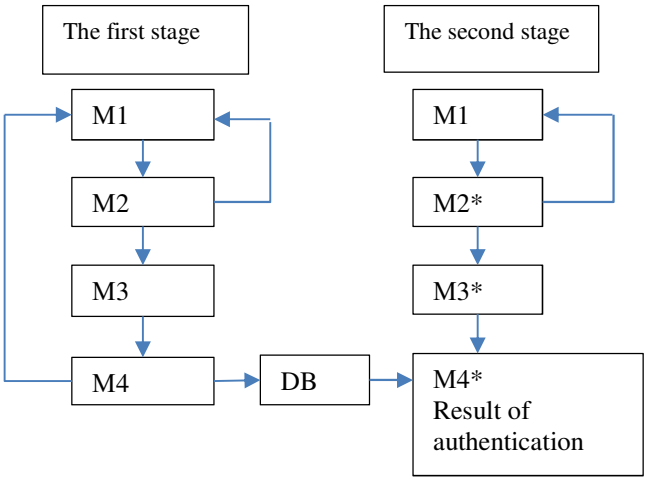

Figure 4. The software part of the authentication system

The M1 software module (current internal noise recording module) is located on each of the electronic devices (part of the client). The following software modules are hosted on the server (part of the server). The work of the software modules is divided into two stages.
In the first stage of the system operation the average template and the authentication threshold for each electronic device are calculated. The following modules are used for this purpose:

- M2 (module for checking the suitability of the current noise record for template formation). Return to M1, if the current record contains a monochromatic interference;
- M3 (module of calculation of autocorrelation functions and templates);
- M4 (module for accumulation of required number of templates and calculation of actual average template and authentication threshold);
- DB Database (database for saving the middle template and authentication threshold).

The second stage of the system is authentication of the electronic device / devices. The following modules are used for this purpose:

- M2* (It is module for checking the suitability of the current noise record for the formation of the current pattern). There is return to M1 if record contains monochromatic interference;
- M3* (It is module of calculation of autocorrelation function on the results of current noise measurement and template);
- M4* (It is module of comparison of current template ED №J and average template ED №J from database DB. Decision making about authentication).

M2…M4 – there is work of modules in the first stage, where M2*… M4* - there is work of modules in the second stage.

The authentication procedure begins with the initiative of electronic device №J, which sends an authentication request to the server. The request contains the ID number of the electronic device. The server returns a response - a request for the current noise record. Electronic device №J runs the program of current recording of internal electrical noise. The result of the program - the data array is sent to the server, where it is further processed. The array must be transmitted to the server using a protocol that ensures the confidentiality of data exchange between the client and the server. Upon receipt by the server of the data set of the current noise recording from electronic device №J, modules M2*, M3* and M4* are executed sequentially. Module M3* is executed under the condition of a positive form factor as a result of the work of M2*. The result (the current noise template of electronic device №J) is transmitted to the M4* module. The database is queried for the electronic device №J template, the data is sent to the M4* module, where they are compared to the current electronic device №J noise template. Authentication result is positive or negative authentication, which is transmitted to electronic device №J.

4.2. The algorithms of the modules

This section describes the algorithms of work of the following modules: M1, M2 (M2*), M3 (M3*), M4, M4*.

The internal electric noise registration module (M1) is a program that is launched by a server command, manages the process of measuring internal electrical noise by an analog-to-digital converter, writes the results to a data array, encrypts the data array, and sends the encrypted array to the server. The block diagram of the algorithm of the M1 module is shown in figure 5.

Input data for the M1 module: recording duration in s; channel of analog-to-digital converter; sampling frequency; the number of bits per one recording sample (ADC bit depth); type of encryption of the data array.

Output data for the M1 module: encrypted time-stamped data array.

The module (M2, M2*) for checking the suitability of the current noise recording for the formation of a template is a program that decrypts the data $S(U(\mathrm{i}))$, rejects the initial part of the noise data array $U(\mathrm{i})$ of length Z, calculates an fragment of autocorrelation function from the reduced array $\tilde{U}(i)$ noise for lags from 0 to R, calculates the distribution of the values of a given fragment of the autocorrelation function, by which it further calculates the form factor FF. If the form factor is positive, then the reduced noise data array $\tilde{U}(i)$ together with the fragment of the autocorrelation function $AC(i)$ of the noise are transmitted to the module M3. If the form factor is not positive, $FF \leq 0$, there is a transition to the module M1 to measure noise again.

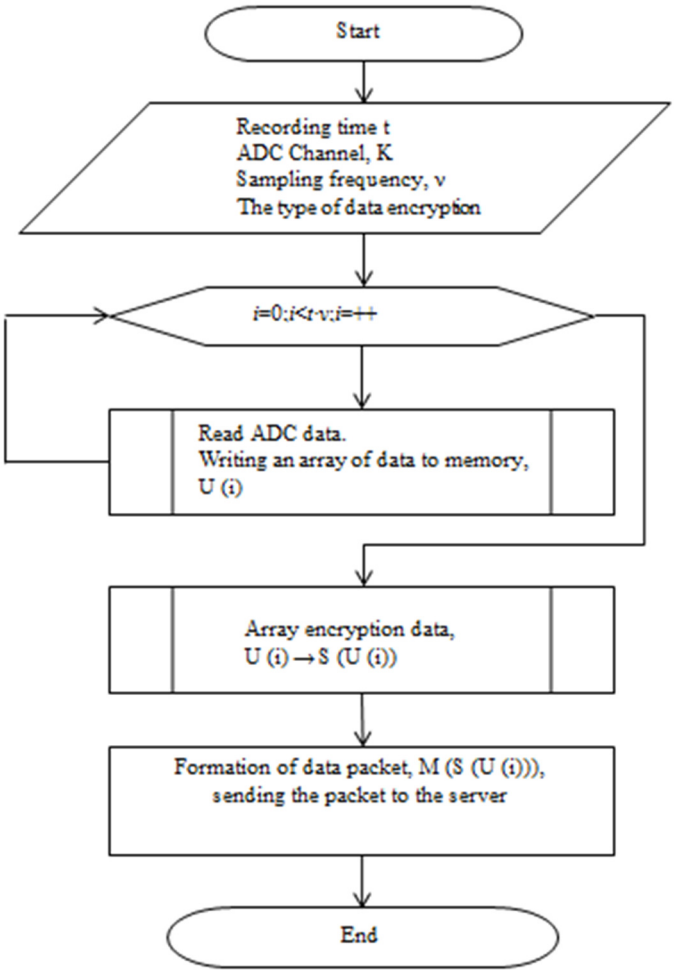

Figure 5. The algorithm of the module M1

The block diagram of the algorithm of operation of the M2 module is shown in figure 6. Input data: encrypted noise data array $S(U(i))$; decryption type S^{-1}.
Output data: an array of noise data $\tilde{U}(i)$; an array of values of the autocorrelation function $AC(\mathrm{i} \leq R)$.

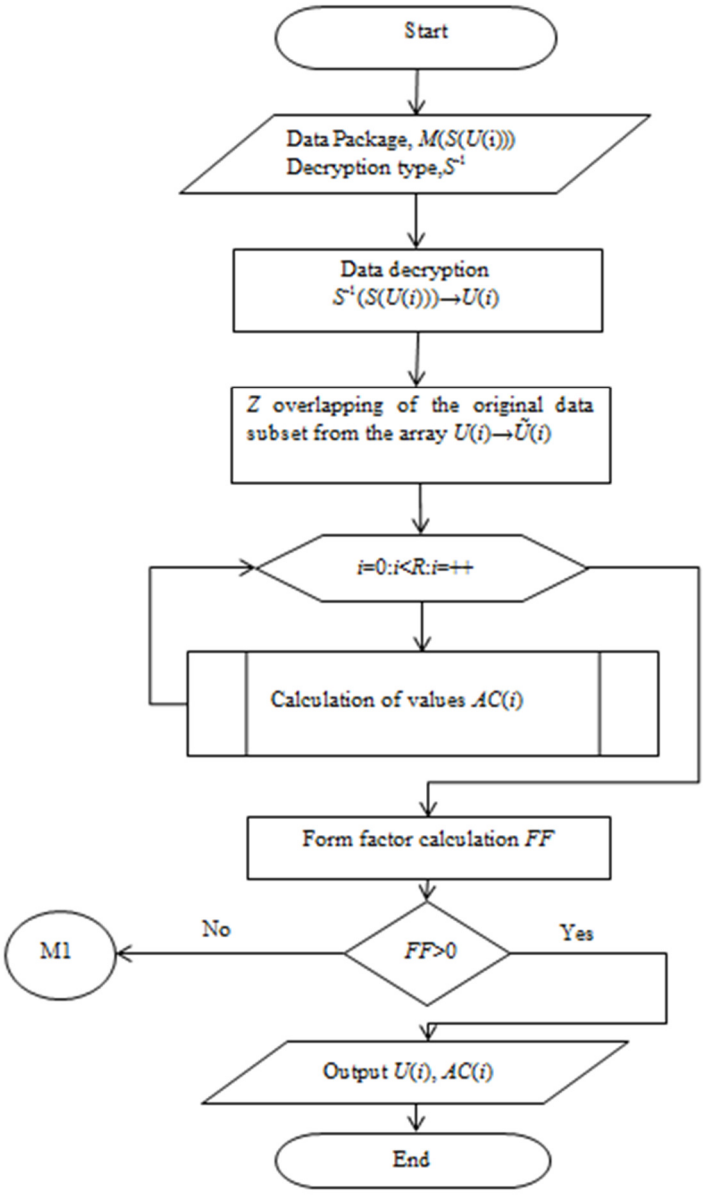

*Figure 6. The algorithm of the module M2 and M2**

The module (M3, M3*) for calculating of the autocorrelation function and of the template is a program in which an authentication template is calculated based on the calculated autocorrelation function of noise.

Input data: the ID number of the computer that is being authenticated. The ID number determines the type of template; an array of noise data $\tilde{U}(i)$; an array of values of the autocorrelation function $AC(i \leq R)$.

Output data: bit template of computer noise with a given ID; autocorrelation function of noise.
The block diagram of the algorithm of operation of the M3, M3* module is shown in figure 7.

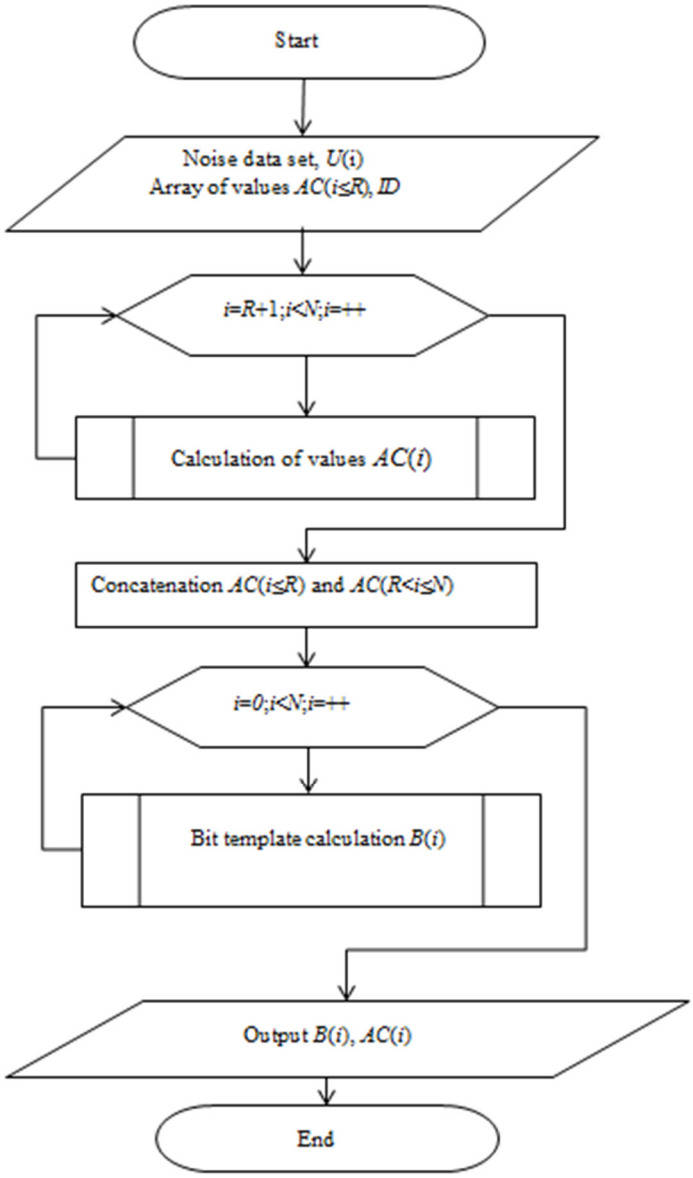

*Figure 7. The algorithm of the module M3 and M3**

The block diagram of the algorithm of operation of the M4 module is shown in Fig 8.

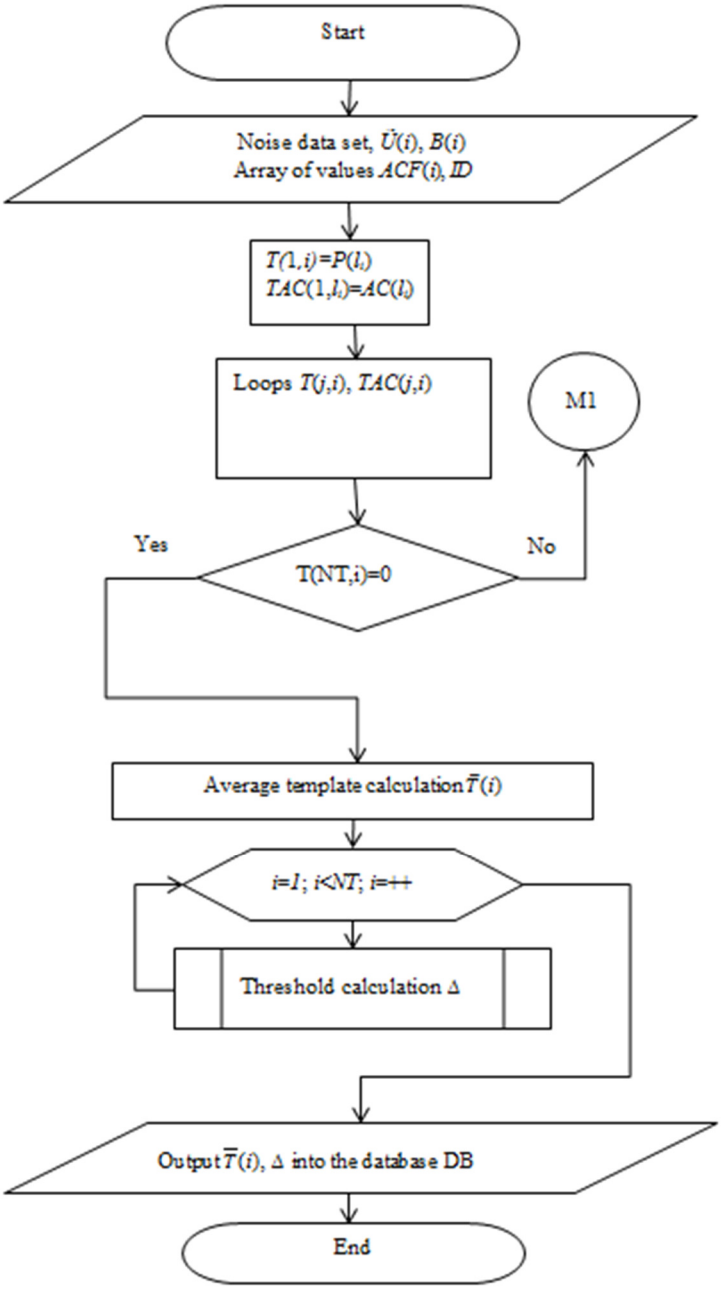

Figure 8. The algorithm of the module M4

The module for calculating the average template and the authentication threshold (M4) is a program that collects N current templates and N autocorrelation functions, calculates the average autocorrelation function as the arithmetic average, and calculates the average template $T(i)$. The authentication threshold Δ is calculated as

the maximum value from the possible distances between the middle pattern and the current patterns.
Input data: arrays of values of the autocorrelation function $AC(i \le R)$, bit template $B(i)$.
Output: average bit template of computer noise; authentication threshold Δ_B.
The block diagram of the algorithm of operation of the M4* module is shown in figure 9.

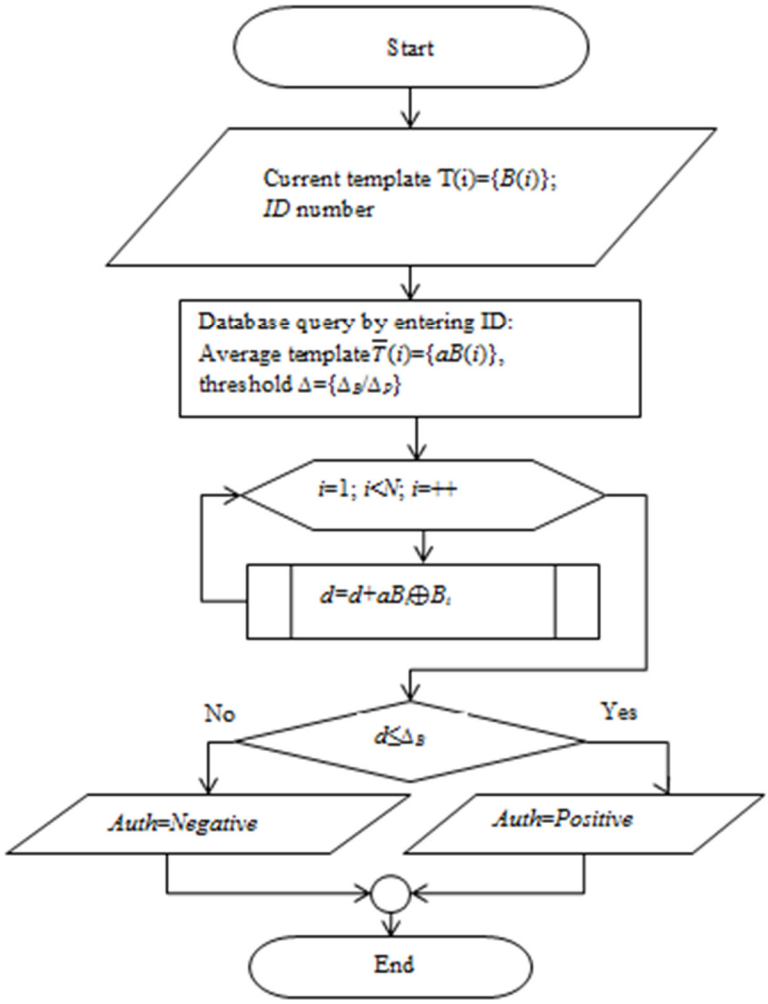

*Figure 9. The algorithm of the module M4**

The authenticity decision module (M4*) is a program in which the distance is calculated between the current noise template of a computer with ID number and the average noise template for a computer with ID number. The calculated distance is compared with the threshold for a computer with ID number. Authentication decision is made.

5. Conclusion

The system allows for continuous auditing of BYOD devices connected to the corporate network, continuous inventory of regular computers, enables authentication of electronic devices of the Internet of Things.
The system does not require the installation of additional equipment, works in automatic mode. Device authentication happens remotely.
Access to the server-side authentication software must be built on role-based access rules, and the authentication template database must be protected. The client part program must be protected from changes.
The implementation of the proposed system will provide a cost-effective authentication solution with high reliability of the result.
Further research will be devoted to the implementation of the proposed system for authentication of one type of the IoT electronic devices.

REFERENCE

1. ROT A., BLAICKE B.: Bezpieczeństwo Internetu Rzeczy. Wybrane Zagrożenia i Sposoby Zabezpieczeń na Przykładzie Systemów Produkcyjnych. Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie, **26** (2017), 188–198.
2. Internet Rzeczy pod ostrzałem cyberprzestępców: *https://alebank.pl/internet-rzeczy-pod-ostrzalem-cyberprzestepcow,* 01.11.2019.
3. Internet Rzeczy czy internet zagrożeń? [ANALIZA]: *https://www.cyberdefence24.pl/internet-rzeczy-czy-internet-zagrozen-analiza,* 25.07.2017
4. RYBALSKY O.V., SOLOVYOV V.I., ZHURAVEL V.V.: The System of tools of examination of audio and videotape recording are in Ukraine. Bulletin of Polotsk State University, Series C, **4**(2018), 15–19. (in Russian)
5. HASSE J., GLOE T., BECK M.: Forensic Identification of GSM Mobile Phones. Proceedings of the first ACM workshop on Information hiding and multimedia security (IH&MMSec'13), Montpellier 2013, 131-140.
6. SVOBODA J., SCHANFEIN M.: Apparatus, System, and Method for Sensor Authentication, United States: Patent Application Publication, 2015, US2015/0006115A1.
7. SAMPLE A., YANG J.: EM-ID: Tag-less identification of electrical devices via electromagnetic emissions. IEEE International Conference on RFID, Orlando 2016, 10 p.
8. SUH E. G., DEVADAS S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation, Proc. of Design Automation Conference, San Diego 2007, 6 p.
9. Toshiba Develops Mutual Authentication Technology for IoT Devices by PUF Fingerprinting Using Variations in Semiconductor Chips: *http://www.toshiba.co.jp/rdc/rd/detail_e/e1806_02.html,* 14.06.2018.

10. NYEMKOVA E., SHANDRA Z., KLOS-WITKOWSKA A., WIECLAW L.: Network Electronic Devices Authentication by Internal Electrical Noise. Computer Information Systems and Industrial Management. Springer, Cham 2018, 474–485.