DOI 10.30898/1684-1719.2020.5.7
УДК 53.083.2

RADIO FREQUENCY IDENTIFICATION AND AUTHENTICATION IN THE CONTROL SYSTEM OF THE MEDICAL DIAGNOSTIC AND TREATMENT PROCESS

S. A. Bagdasaryan [1], V. I. Nikolaev [1], E. R. Pavlyukova [2], S. O. Nikolaeva [1]

[1] Research and Production Enterprise "Radio Frequency Identification Technologies for Communications", 4 (1), Sukharevskiy Pereulok, 4-1, Moscow 127051, Russia
[2] Kotelnikov Institute of Radioengineering and Electronics of RAS, Mokhovaya Str., 11-7, Moscow 125009, Russia

The paper is received on May 7, 2020

Abstract. The problem of providing security of the systems for medical treatment and diagnostic process control (SMTDC) based on radio frequency identification with the application of surface acoustic wave technologies in the approximation of the absence of collisions of tag responses is in the focus of this research. Using the statistical theory for detecting and differentiation of M signals with an unknown temporal position at the fading channel output, we have determined the characteristics of the simultaneous detection and differentiation of the responses by SAW sensors of biological signals and patient parameters and SAW radio frequency tags to the polling signal over a large a priori interval containing significant number of delay resolution elements. The approach for solving of the problems on identification of biological signals and patient parameters, as well as authentication of the patient and the attending physician to increase the security of telecommunication systems MTDC. The significant advantages of SAW technology in solving these problems are demonstrated.

Keywords: RFID, authentication, secure access to information networks, diagnostic and treatment process, patient biological signals and indicators.

Introduction

Taking into account actual safety requirements and trends in the construction and development of monitoring systems for the patient's current state [1,2], there is the problem of their security maximizing associated with providing highly reliable

identification of various diseases dangerous to the patient's life and their complications. at the early stages, as well as patient authentication with the simultaneous authentication of the attending physician, who has access to confidential information at all stages of the diagnosis and treatment of the patient. To solve the problems, in our opinion, it is reasonable to use systems of radio frequency identification (RFI) [3,4] and authentication [5] based on the technologies of surface acoustic waves (SAW), having a high degree of security from cloning [6] as distinct from the other known technologies.

In the problem on identifying of biological signals and patient indicators (SAW-sensor-tag), as well as authentication of the patient and the attending physician (-tag) based on these systems, we assume that one of the M sensor tags is located in the polling area, or there is no such tag sensors. Therefore, the system reader should carry out the following procedures jointly: detection of signal responses from the sensor-tags on polling pulse and assessment of its information parameters, including biological signals and patient indicators. The aspects of synthesis and analysis for similar devices were considered in detail earlier in relation to detecting-distinguishing problem for signals with an unknown arrival time in asynchronous communication systems in the presence of fading [7,8]. However, the application of this approach in RFI systems has its own peculiarities due to the structure of SAW devices (sensors and tags) allowing to realize wave delays with the order of several nanoseconds and responses modulated simultaneously in amplitude and phase.

In this regard, it is of considerable interest to evaluate the probabilistic characteristics of SAW devices to provide highly reliable identification of diseases and authentication of participants (patient and doctor) of treatment and diagnosis processes.

Providing highly reliable identification of diseases and authentication of participants in the SMTDC

The goal of the present research was to study the information parameters and characteristics of radio frequency identification and authentication based on SAW in SMTDC.

In the SAW sensors and tags under data transmission it is possible to encode the data, both in amplitude and phase, using different types of polling signals, in particular phase-shift signals (PMS), which is associated with the features and physical principles of operation of the SAW structure of sensors and tags. Based on this, it is possible to implement secure access to the resources of the SMTDC using the procedures for identification and authentication of the identity of the attending person using a SAW tag to determine authority.

Let us consider in more detail the implementation of identification and authentication procedures in RFI systems based on SAW. At the first stage, the tag identification is carried out by sending a polling impulse to the radio frequency tag on the SAW. The polling impulse is a segment of a sinusoid with the duration $\tau_\Delta = 5...10$ ns and frequency $f_0 = 2,45$ GHz [8, 9]:

$$\delta_s(t) = \begin{cases} A_0 \sin(2\pi f_0 t), \ 0 \le t \le \tau_\Delta, \\ 0, \ t < 0, t > \tau_\Delta. \end{cases} \quad (1)$$

As a result of interaction of polling impulse $\delta_s(t)$ with m-th tag ($m = \overline{1,M}$) the tag response is formed as follows [8]

$$s_m(t) = \int_{-\infty}^{\infty} h_m(\tau)\delta_s(t-\tau)d\tau, \quad (2)$$

where

$$h_m(t) = \sum_{k=1}^{N} A_{mk} E_{mk}(t-\tau_{mk}) \sin[\omega_{mk}(t-\tau_{mk}) + \theta_{mk}], \quad (3)$$

– impulse characteristic of m-th tag [8]; N is the number defining the tag information capacity (a number of pulses of the tag code sequence); A_{mk} is an amplitude of k-th impulse of m-th tag; $E_{mk}(t)$ is an envelope of k-th impulse of m-th tag; τ_{mk} is the time delay up to the centre of k-th impulse of m-th tag; ω_{mk} is an angular central frequency of radio frequency filling by k-th impulse of m-th tag; θ_{mk} is initial phase of radio frequency filling by k-th impulse of m-th tag. It should be emphasized that due to the fading caused by the multi-beam type of the tag response propagation, as well as the scatter of the possible tag locations within the polling

area, the amplitude, initial phase and time of arrival of the response (2) at the input of the reader will be unknown. Therefore, the response processing algorithm (2) must take into account the indicated feature of the response signals and can be synthesized on the base of the methods developed in [7, 10].

Let us consider on time interval $[0,T]$ the random process realization:

$$x(t)=\begin{cases} n(t), \\ s_m(t,\tau_{0m},A_m,\varphi_m)+n(t),\ m=\overline{1,M}, \end{cases} \quad (4)$$

here + – stationary Gaussian noise with zero mean and correlation function $K_n(t_1-t_2)$; $\tau_{0m}\in[T_1,T_2]$ – unknown time position of tag response, moreover the region $[T_1,T_2]$ contains many elements of delay resolution. In accordance with the formula (4), we assume that in the observed data there is either no response from the tag, or there is a response from one of the tags (the case of collisions, when several tags can respond to the polling pulse right away, is not considered in present paper).

In the general case, the tag response like in [7], could be presented by the following way:

$$s(t,\tau,A,\varphi)=A\big(f(t-\tau)\cos[\omega t+\psi(t,\tau)-\varphi]+g(t-\tau)\sin[\omega t+\chi(t,\tau)-\varphi]\big). \quad (5)$$

Here, to simplify formula writing, the index m is omitted. In the expression (5) $\{f(t),\psi(t)\}$, $\{g(t),\chi(t)\}$ are the laws of amplitude-phase modulation of the tag response quadrature; A, φ – unknown due to fading amplitudes and initial phases of tag responses.

Let us introduce the following designation: $\pi_c=A\cos\varphi$, $\pi_s=A\sin\varphi$, as well as

$$\begin{aligned} U_c(t,\tau)&=f(t-\tau)\cos[\omega t+\psi(t,\tau)]+g(t-\tau)\sin[\omega t+\chi(t,\tau)], \\ U_s(t,\tau)&=f(t-\tau)\sin[\omega t+\psi(t,\tau)]-g(t-\tau)\cos[\omega t+\chi(t,\tau)]. \end{aligned} \quad (6)$$

Then based on our research results [7] likelihood ratio functional (LRF) for tag response parameters (5) it is possible to write as

$$\Lambda(\tau,\pi_c,\pi_s)=\exp[\pi_c X(\tau)+\pi_s Y(\tau)-(\pi_c^2+\pi_s^2)q_0^2/2]. \quad (7)$$

here

$$X(\tau)=\iint x(t_1)U_c(t_2,\tau)\theta(t_1,t_2)dt_1dt_2,\ Y(\tau)=\iint x(t_1)U_s(t_2,\tau)\theta(t_1,t_2)dt_1dt_2 \qquad (8)$$

– quadrature components of the reader linear part; $\theta(t_1,t_2)$ – inverse correlation function determined by the solution of the integral equation $\int_0^T K_n(t_1-t)\theta(t,t_2)dt=\delta(t_1-t_2)$; $\delta(\cdot)$ – delta function. Parameter q_0^2 makes sense of the signal-to-noise ratio for the signal (5) under $A=1$:

$$q_0^2=\iint U_c(t_1,\tau)U_c(t_2,\tau)\theta(t_1,t_2)dt_1dt_2=\iint U_s(t_1,\tau)U_s(t_2,\tau)\theta(t_1,t_2)dt_1dt_2.$$

The application of the Bayesian approach to the synthesis of the algorithm for the simultaneous detection-differentiation of tag responses leads to the following asymptotically quasi-optimal (with an increase in the signal-to-noise ratio ($z_m^2=A_m^2q_0^2$) decision making rule [7, 10]: process realization (4) contains *m*-th tag response, if inequalities hold simultaneously

$$\begin{aligned}&\max L_m(\tau_{0m})>h,\\&\max L_m(\tau_{0m})>\max L_k(\tau_{0k}),\\&k,m=\overline{1,M},\end{aligned} \qquad (9)$$

where $L_m(\tau_{0m})=\ln(\Lambda_m(\tau_{0m}))$, and $\Lambda_m(\tau_{0m})=\exp[(X_m^2(\tau_{0m})+Y_m^2(\tau_{0m}))/2q_0^2]$ – maximized on parameters (π_{cm},π_{sm}) LRF (7); h – threshold whose value is determined by a given optimality criterion. From the expressions (9) it follows that at first it is necessary to find the absolute maxima of the LRF logarithms for all possible responses from the M tags and compare with a certain threshold h. Then the decision regarding the response from *m*-th tag in the process realization (4) is making while satisfying both inequalities (9). If $\max L_m(\tau_{0m})<h,\ m=\overline{1,M}$, then a decision is made that there is no response from any tag in the process realization (4) and therefore the tag itself in the polling area.

Definition of the characteristics of the joint detection-differentiation algorithm for fading tag responses (9) with an unknown arrival time is based on the application of the theory of runs for random processes. Such approach gives more simple and more accurate results than the other methods [7, 10]. Assuming that the a priori

probabilities of tags appearing inside the polling area are the same and using the approximation for the distribution of the logarithm absolute maximum of the LRF $L_m(\tau_{0m})$ from [10], based on research results [7] we could write the following formulas for the algorithm characteristics (9):

the probability of false alarm under detecting tag responses

$$\alpha = 1 - \exp\left(-\frac{\xi M \sqrt{h}}{\sqrt{\pi}} \exp(-h) \right), \tag{10}$$

the average probability of tag response failure

$$\begin{aligned} \beta = {} & \frac{1}{M} \exp\left(-\frac{\xi M \sqrt{h}}{\sqrt{\pi}} \exp(-u) \right) \int_0^h \exp(-u - 0{,}5z^2) I_0\left(z\sqrt{2u} \right) du + \\ & + \left(1 - \frac{1}{M} \right) \int_0^h \exp\left[-u - 0{,}5z^2 - \frac{\xi M \sqrt{u}}{\sqrt{\pi}} \exp(-u) \right] I_0\left(z\sqrt{2u} \right) du, \end{aligned} \tag{11}$$

the average probability of tag response differentiation error

$$\begin{aligned} P_e = {} & \left(1 - \frac{1}{M} \right) \left(1 - \int_h^\infty \exp\left[-u - 0{,}5z^2 - \frac{\xi M \sqrt{u}}{\sqrt{\pi}} \exp(-u) \right] I_0\left(z\sqrt{2u} \right) du \right) + \\ & + \frac{1}{M} \exp\left(-\frac{\xi M \sqrt{h}}{\sqrt{\pi}} \exp(-u) \right) \int_0^h \exp(-u - 0{,}5z^2) I_0\left(z\sqrt{2u} \right) du, \end{aligned} \tag{12}$$

where ξ – reduced length of prior interval $[T_1, T_2]$, having sense of the number of signal resolution elements on this interval; $z^2 = A^2 q_0^2$ – signal-to-noise ratio; $I_0(\cdot)$ - modified zero-order Bessel function of the first kind.

At the Fig. 1 there are presented the dependencies of the average probability of tag response failure β on signal-to-noise ratio z, obtained using formula (11) for tag number M, equal to 10, 100, 1000 and 10000. The threshold value h was selected based on the Neumann-Pearson criterion [11] using formula (10) for two false alarm probability values $\alpha = 0{,}01$ and $\alpha = 0{,}001$ with $\xi = 50$. The calculated threshold value are presented at the Table.

At Fig. 2 there are presented the dependencies of the average probability of tag differentiation error P_e on signal-to-noise ratio z, obtained with the formula (12) for

the tag number M, equal 10, 100, 1000 and 10000. Under calculations of P_e the same threshold values h were used as in the case of the average probability of tag response failure β (see Table).

Table.

α	0,01				0,001			
M	10	100	1000	10000	10	100	1000	10000
h	11,46	13,86	16,24	18,61	13,86	16,24	18,62	20,98

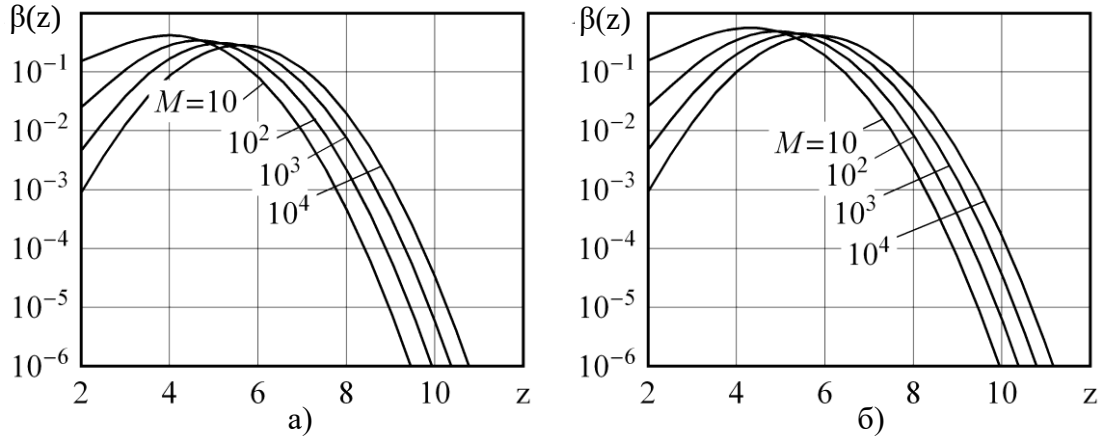

Fig. 1. The dependence of the average probability of the tag response failure at the identification stage on the signal-to-noise ratio for a different number of tags in the set for two false alarm probability values: a) $\alpha = 0,01$ and b) $\alpha = 0,001$.

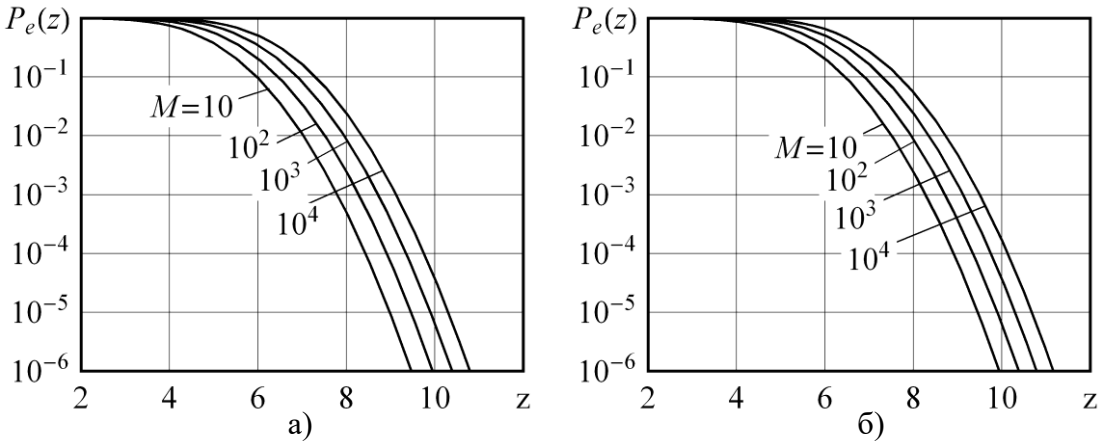

Fig. 2. The dependence of the average tag differentiation error rate on the signal-to-noise ratio with a different number of tags in the set for two false alert probability values: a) $\alpha = 0,01$ and b) $\alpha = 0,001$.

Analysis of the curves at Fig. 1 and Fig. 2 allows us to conclude that the energy efficiency of detecting/differentiation of tag responses, as could be expected,

decreases with an increasing in the number of tags in the set. Besides, we can see from Fig. 1, that the dependence of the average probability of tag response failure $\beta(z)$ is a nonmonotonic function of signal-to-noise ratio. This is due to the features of signal search at large a priori intervals $[T_1, T_2]$ [5, 10]. Under noise increasing (reducing of signal-to noise ratio z) initially, there is an increase in the probability of signal failure. However, with a sufficiently large noise power, outliers of the noise function for statistics $L(\tau)$ begin to play an increasingly important role in that part of the a priori interval where there is no peak of the signal function (so called anomalous errors). This leads to an increase in the probability of threshold exceeding, i.e. reduction in probability of the signal failure. Now let us consider the tag authentication procedure (second stage).

At the second stage in case of successful identification procedure for *m*-th tag (based on algorithm (9)) from data base the complex polling signal by the following type is selected and radiated:

$$s'_m(t) = \sum_{k=1}^{K} a_k h_m(kT_s - t), \qquad (13)$$

where $a_1, ..., a_K$ is pseudorandom code, the elements of which take the values ± 1; $h_m(t)$ – impulse characteristic of *m*-th tag (3); T_s – duration of tag impulse characteristics. As an example at Fig. 3 there is presented the normalized complex envelope of tag impulse characteristic (3), containing 10 impulses with the envelope $E(t) = \mathrm{sinc}(\pi t / \tau_0)$, the amplitudes of which take the code values $\{1;1;1;1;0;1;1;0;1;1\}$, and initial phases of radio frequency filling – the values $\{0,0,0,\pi,0,\pi,0,0,\pi,0\}$ respectively. Complex envelope of polling signal (13), corresponding to presented at Fig. 3 complex envelope of impulse characteristic $h_m(t)$, is demonstrated at the Fig. 4. In given case pseudorandom code $a_1, ..., a_K$ defined as $\{1,-1,-1,1\}$. Normalized complex envelope of tag response on polling signal (13) is presented at the Fig. 5. Time period at the Fig. 3 – 5 represented in counts.

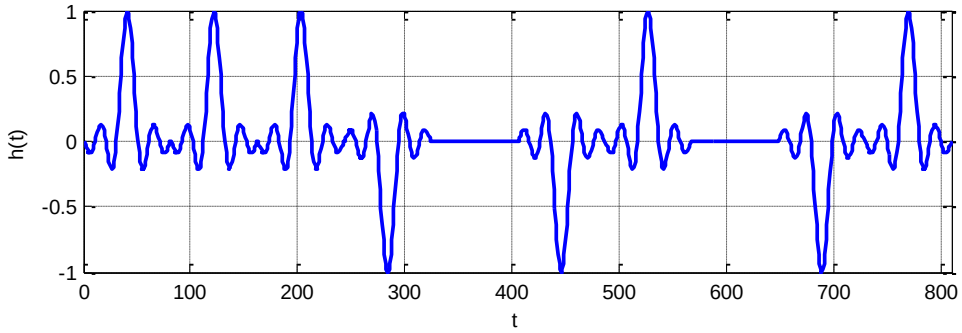

Fig. 3. Example of complex envelope of tag impulse characteristic $h_m(t)$.

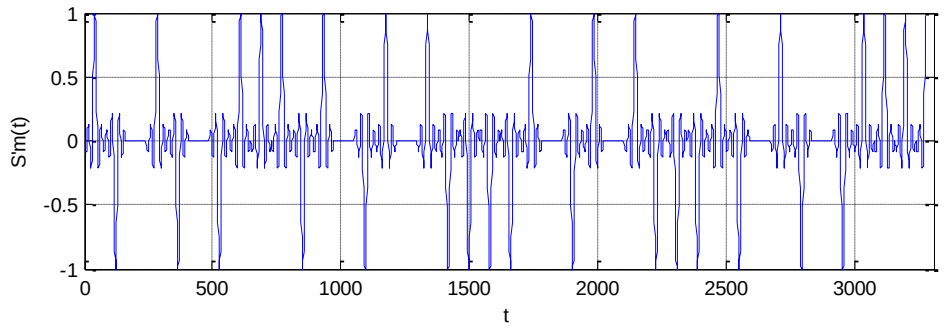

Fig. 4. Complex polling tag signal $s'_m(t)$ with the code $\{1,-1,-1,1\}$.

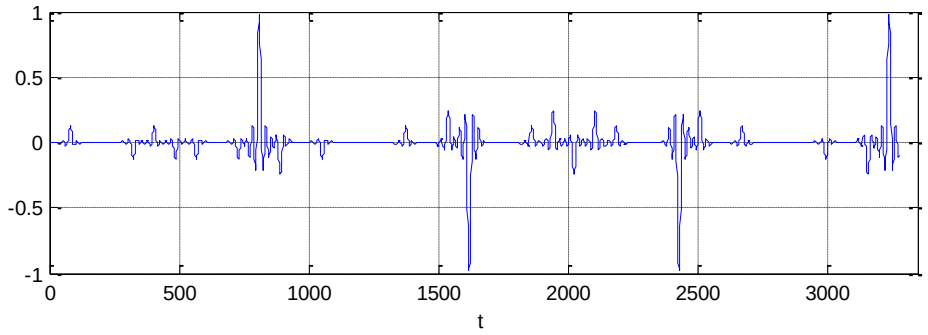

Fig. 5. Normalized envelope for tag response on polling signal $s'_m(t)$ with the code $\{1,-1,-1,1\}$.

Thus, during the tag authentication procedure, we verify the authenticity of the tag, since the tag responds by a certain way to a complex polling signal (13) (by convolution of the input signal (13) with the impulse characteristic (3)). Herewith the polling signal code (13) $a_1,...,a_K$ could be varied by pseudorandom way from survey to survey, making difficult the falsification of tag response on polling signal (13). Here it is appropriate to make the following analogy with the cryptosystem. We have «public key» that is polling pulse (1) and «private key» that is the complex polling signal (13), developing in dependence to selected code $a_1,...,a_K$ and taking into account the tag response at the authentication stage.

In order to make fake tag code, an attacker needs to read the polling impulse (1) and response by tag on this impulse, and then, using obtained impulse characteristic, to synthesize a device that has a given impulse characteristic. At present, practically there is no possibility to develop a device with SAW-tag impulse characteristic based on semiconductor technologies. This is due to the following features:

1) Tag operating frequency – 2,45 GHz, in given range it realize the delays of the order of one nanosecond;
2) limited functionality of the actual element base;
3) analysis procedure for tag impulse characteristic by an attacker is further complicated by the multi-beam propagation mode of the tag response.

Conclusion

Based on the above mentioned, we can make conclusion about nonrealizability of the device based on semiconductor technologies. So, the possibility for an attacker to read the polling and response signals of the tag at the stage of identification and authentication exists.

Whereas in order to solve a similar problem in the SAW technique, a high-tech logical set will be required, including a reader, technical documentation, topologies of sensors and tags and equipment for the manufacture of a precision photomask and a SAW element of a tag. The high cost of the noted equipment and the services to organize this manufacturing have not profitable interest for the cloning of SAW devices. In addition, in our case, the polling signal can be changed by pseudo-random way from request to request; the fact that anybody knows the tag response even on a complex signal does not provide making fake tag response promptly under the present hardware capabilities.

This research have been executed under financial support by RFBR: grant № 18-29-02076.

References

1. Bagdasaryan A.S., Bagdasaryan S.A., Nikolaev V.I., Kashchenko O.V., Nikolaeva S.O., Pavlyukova E.R. Wireless monitoring for biological signals by cardio-vascular system of patient. *Zhurnal Radioelektroniki - Journal of Radio Electronics*. 2019. No. 6. Available at http://jre.cplire.ru/jre/jun19/13/text.pdf DOI 110.30898/1684-1719.2019.6.13 (In Russian)
2. Bagdasaryan A.S., Bagdasaryan S.A. Information technologies using radiomonitoring in general medical practice. *Fundamental'nyye problemy radioelektronnogo priborostroyeniya - Fundamental problems of radioelectronic instrumentation*". 2018. Vol. 18. No.3. P. 521-525 (In Russian)
3. Bagdasaryan S.A., Gulyaev Yu.V. Acoustoelectronic technologies in radio frequency identification. *Izvestiya Vysshikh Uchebnykh Zavedenii Rossii. Radioelektronika - Journal of the Russian Universities. Radioelectronics*. 2005. Vol. 4. P. 24 (In Russian)
4. Bagdasaryan A., Bagdasaryan S., Dneprovskiy V., Karapetiyan G., Nikolaeva S. Compact radio frequency identification tags on SAW for functional capability extension. *Elektronika: nauka, tekhnologiya, biznes - Electronics: Science, Technology, Business*. 2014. Vol. 3 (134). P. 70-76. (In Russian)
5. Gulyaev Yu.V., Bagdasaryan A.S., Kashchenko G.A., Bagdasaryan S.A., Semenov R.V. Authentication in wireless LANs based on RFID devices. *Informatsiya i bezopasnost' - Information and Security*. 2007. Vol. 10. No. 3. P. 395-402 (In Russian)
6. Bagdasaryan S.A., Kashchenko G.A., Semenov R.V. Potential structural security analysis for answering signals and response signals of tags on SAW to increase telecommunication system security. *Sistemy i sredstva svyazi, televideniya i radioveshchaniya -. Systems and tools for communication, television and radio broadcasting*. 2011. Vol. 1-2. P. 156-160. (In Russian)
7. Radchenko Y.S., Radchenko T.A. Signal detection-differentiation in asynchronous communication systems in the presence of fading. *Journal of*

Communications Technology and Electronics. 2003. Vol. 48. No.5. P.526–531.

8. Hartman C.S. A Global SAW ID Tag with Large Data Capacity. *Proc. IEEE Ultrasonics Symposium*, Munich. 2002. P. 63-67.
9. Hartman C.S., Brown P., Bellamy J. Design of Global SAW RFID Tag Devices. *Proceedings of Second Int. Symp. on Acoustic Wave Devices for Future Mobile Communication Systems*. Chiba Univ., Japan. March 2004.
10. Trifonov A.P., Shinakov Y.S. *Sovmestnoye razlicheniye signalov i otsenka ikh parametrov na fone pomekh* [Common signal differentiation and estimation of signal parameters against a background of interference]. Moscow, Radio i Svyaz Publ. 1986. 264 p. (In Russian)
11. Tikhonov V.I. *Statisticheskaya radiotekhnika* [Statistical Radio Engineering] Moscow, Sovetskoye Radio Publ. 1966. 680 p. (In Russian)

For citation:
Bagdasaryan S.A., Nikolaev V.I., Pavlyukova E.R., Nikolaeva S.O. Radio frequency identification and authentication in control system for diagnostic and treatment process. *Zhurnal Radioelektroniki - Journal of Radio Electronics.* 2020. No. 5. Available at http://jre.cplire.ru/jre/may20/7/text.pdf. DOI 10.30898/1684-1719.2020.5.7