Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning

Hennadii Hulak[a,c], Larysa Kriuchkova[b], Pavlo Skladannyi[c], and Ivan Opirskyy[d]

[a] *Institute of Mathematical Machines and Systems Problems of the Ukraine National Academy of Science, 42 Academician Glushkov ave., Kyiv, 03187, Ukraine*
[b] *State University of Telecommunications, 7 Solomenskaya str., Kyiv, 03110, Ukraine*
[c] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[d] *Lviv Polytechnic National University, 12 Stepana Bandery stκ, Lviv, 79000, Ukraine*

Abstract

The paper investigates the problem of building protected guarantee systems of distance learning in higher education institutions. The requirements for the electronic record book are formed. The generalized scheme of interaction of components of the RFID system with inductive communication is presented, as well as the block diagram of the generalized algorithm of information support of the educational process of higher education institutions by the ERB identification system.

Keywords

Information system, distance learning, RFID system, higher education institutions, electronic record book.

1. Introduction

The study of the problems of building in higher education institutions (HEI) protected guaranteed distance learning systems that would meet the requirements of the law [1], indicates the need to create a virtual learning environment, which is the basis of the information system of distance learning (ISDN) [2]. Its components in essence are electronic analogues of the usual material components of the educational process. In particular, they are as follows:

- Corporate repositories of knowledge and resources, including educational information electronic resources, libraries of various applied educational programs, modeling complexes, etc.
- Databases of organizational and planning documents and methodological support of the educational process (curricula and programs, class schedules, working programs of academic disciplines, methodological complexes for conducting classes, etc.).
- Individual and group documents of accounting of results of the educational process (record books, journals of the account of classes of educational groups, etc.).
- Documents of current quality control of mastering learning programs (test papers, tests, essays, course papers, dissertations, etc.).

To ensure high quality of distance learning, each electronic analogue of the usual essence, among the components listed above, must meet the requirements of regulations on higher education and best international practices defined in international standards. The same applies to the paper record book of the higher education applicant, which now actually performs the functions of his or her visual identification and accumulation of data on the implementation of measures for the current control of the acquired knowledge. The creation of its electronic analogue "Electronic record book" (ERB), taking into account the principles of building a system of distance learning of the higher education institution (HEI), set out in the work [2], will implement such basic functions as:

- Two-factor authentication of the student in the protected guaranteed system of HEI.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: hulak@ukr.net (A.1); alara54@ukr.net (B.2); p.skladannyi@kubg.edu.ua (C.3); iopirsky@gmail.com (D.4)
ORCID: 0000-0001-9131-9233 (A.1); 0000-0002-8509-6659 (B.2); 0000-0002-7775-6039 (C.3); 0000-0002-8461-8996 (D.4)


- Unauthorized access protection (UAP) to data stored in the ERB.
- Data storage of current (test papers, tests, essays, coursework, etc.) and semester (tests, exams) control of knowledge.
- Ensuring the accounting of the actual study time during access to the ISDN within the framework determined by the schedule of classes.
- Formation/verification of the student's electronic signature and verification of the teacher's signature only upon presentation of a public key certificate by both of them (each current control document stored in the ERB must be signed by both the teacher and the student).
- Encryption of confidential information/data in the ERB using a symmetric algorithm key, which is generated and stored in the ERB without the possibility of its extraction (to decrypt the data, a recovery procedure based on 2 keys out of 3, for example, from the set {the student, the head of educational and methodical department, dean}).
- Creation of an encryption session key for remote access to the HEI server using the open key distribution protocol (each block of data sent by one of the participants to the other must be protected by the MAC message authentication code).

To do this, a rational solution would be to use in the ERB: international standards, such as AES, RSA, or MD5 to ensure appropriate cryptographic transformations; modern interfaces such as USB, Bluetooth, or Wi-Fi to interact with a variety of computer devices, including laptops, tablets or smartphones; electronic signature technologies in order to ensure the storage of ERB copies for a certain period on the HEI server, which will have legal force [3] and will allow, if necessary, to renew documents on higher education; RFID technology to enable rapid identification of ERB devices, etc.

The task of creating an ERB with all the above elements will be to choose from a set of possible options such variant of an ERB identification system, which would provide reliable identification of "The electronic record book" of a given quality with minimal capital and operating costs.

2. Introduction

The most important part of this identification system is its primary measuring transducer (PMT), which must have a high speed, be sensitive to the primary informative parameter and ensure the stability of the characteristics under the influence of destabilizing factors [4]. These characteristics are closely interrelated. And the improvement of one of them usually leads to the deterioration of others. Thus, increasing the accuracy of measuring the informative parameter will reduce the speed, and vice versa, increasing the speed of the PMT reduces the accuracy of measurement. Since accuracy is an economic category (i.e., the more accurately the informative parameter is measured, the more efficiently the obtained information can be used, but the cost of obtaining it increases), when creating an ERB identification system it is necessary to solve the compromise problem of choosing the optimal ratios of all parameters. Possible methods of its solution are:

- Mathematical modeling of the ERB identification system. Its advantage is the ability to evaluate the static and dynamic characteristics of such systems. The limitation is due to the fact that the degree of reliability of the models depends on the practical and theoretical experience of their developers.
- Formation and research of generalized indicators of the ERB identification system using graphoanalytical method, "progressive standard" method, etc. The advantage of these methods is the ability to take into account a large number of partial indicators of a single numerical characteristic—a generalized indicator, which allows a fairly simple comparative evaluation of such systems. The limitations are due to the fact that these methods do not take into account some economic and production factors.
- Application of expert evaluation methods based on the use of generalized human experience—so-called "collective wisdom."

In this case, the methods of expert evaluation are considered decisive in solving complex problems of evaluation and selection of any objects as well as in the analysis and forecasting of situations with a large number of significant factors. They are used, as a rule, provided that "the selection, justification, and evaluation of the results of decisions cannot be performed on the basis of accurate calculations. This ensures the active and purposeful participation of specialists at all stages of decision-making, which allows to significantly improve their quality and efficiency" [5]. Expert methods provide an

opportunity to study more deeply the phenomena that are poorly studied by other methods, as well as to identify the most important and significant elements, without omitting the details and relationships, without which a model of the problem cannot be built. The main disadvantages of the methods are the subjectivity of experts' opinions in the sought-after assessments and the limits of their judgments. The main advantage of these methods, given the small requirements for the availability of a priori information about the object of study, is the relative simplicity and ease of use to predict almost any situation.

In the experts` opinion, the main indicator for assessing the quality of the ERB identification system is, as a rule, the reliability of the identification results. It is expressed by the probability of correct identification of the ERB. The legitimacy of the probabilistic approach in assessing the quality of the identification system is explained by the random nature of the processes occurring in an identification, when due to destabilizing factors and random external perturbations the parameters of both measuring instruments and ERB identification features are being changed. The results of identification are considered as random events, with a certain probability corresponding to the real identifying features of the ERB.

In view of the above, the most acceptable for the identification of the ERB is RFID technology with inductive coupling, which uses passive electric oscillating circuits (PEOC) as identification features. Actually, the ERB identification system itself should consist of (Fig. 1):

- The ERB kit with the carriers of identification marks.
- Readers with a transceiver interface for communication with ERB code carriers located in the identification area.
- The application installed on the computer (tablet).

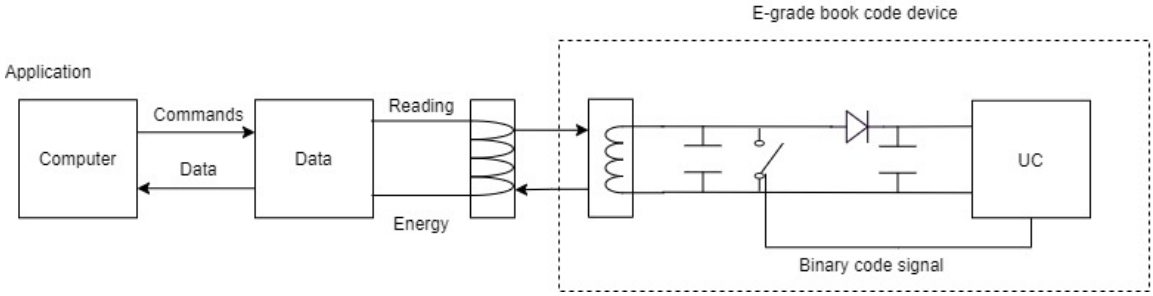

Figure 1: Generalized scheme of interaction of components of RFID system with inductive coupling

Tasks of the reader are the following: activate the code carrier brought in an identification zone; to receive the identification number of the carrier with the subsequent transfer to the computer. The primary measuring transducer (PMT) in RFID technology with inductive coupling is an electrical oscillating circuit tuned in resonance to the frequency of the supply generator. A sensitive element of PMT is the inductance made in the form of a frame. The PMT output voltage amplitude is used as an informative parameter of PMT. Upon entering the identification area, the PEOC, the tuning frequency of which coincides with the frequency of the electromagnetic field of the reader, takes the energy of this field. Thus, passive RFID tags with a chip receive energy for operation

The ERB identification code is generated by switching (shorting) the PEOC in accordance with the assigned code (so-called load modulation).

Processing of input information and generation of the corresponding signal is provided by a silicon CSMOS chip (a chip of complementary structure “metal-oxide-semiconductor”). The choice of CSMOS chip—semiconductor technology for the construction of integrated circuits is explained by close to zero power consumption in the static state. The scheme of interaction of PMT and PEOC is presented in Fig. 2.

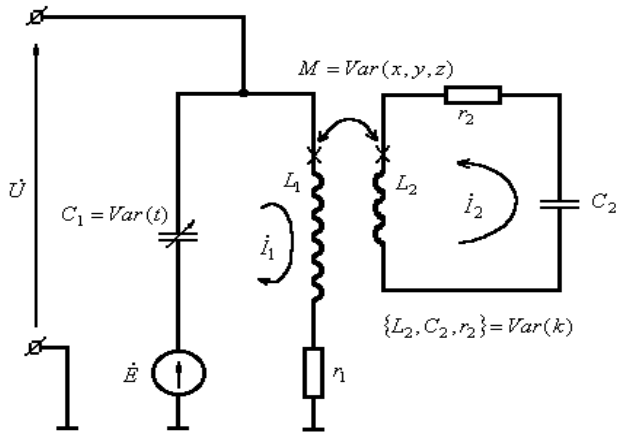

Figure 2: The scheme of interaction of the contour of the source of the field and PEOC: L_1 is the source of the field; L_1C_1 is the field source outline; $\dot{E}$ is voltage generator, feeding the field source outline; L_2C_2 is PEOC; $\dot{U}$ is the informative parameter; M is the coefficient of mutual induction between the coils L_1 and L_2; x, y, z are the coordinates of the PEC application; k is the field of the frequency values of the PEOC setting

The mathematical model of the process of interaction of PMT with PEOC of the object can be represented as follows [6]:

$$\dot{U} = \dot{E}\frac{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_{L_1} - \frac{w^2M^2}{|z_2|^2}x_{2)}}{(r_1 + \frac{w^2M^2}{|z_2|^2}r_2) + j(x_1 - \frac{w^2M^2}{|z_2|^2}x_{2)}} \quad (1)$$

where r1 and r2 – own losses in the contour of the field source and PEOC;

$$Z_1 = r_1 + j(\omega L_1 - \frac{1}{\omega C_1}) \text{ и } \quad Z_2 = r_2 + j(\omega L_2 - \frac{1}{\omega C_2})$$

is complex resistance of each of the circuits; $\dot{E}$ ω - the circular frequency of the EMF source E

The maximum reading radius R is limited by the value of the near zone of the electromagnetic field: $R < \lambda / 2\pi$ where λ is the wavelength of the electromagnetic field generated by the field source. Analysis of expression (1) shows that the change in voltage at the field source is determined by the change in denominator. Increasing the active resistance of the field source circuit leads to a decrease in the voltage at the field source L1. Thus, by reducing the voltage at the field source caused by an increase in irreversible energy losses, we can judge about the presence of PEOC at the object, the tuning frequency of which coincides with the field frequency (Fig. 2).

PEOC "works" when the residual value of the informative parameter reaches a controlled level. The zone of selection of the controlled level of the informative parameteris set by the reference (threshold) value of the comparator voltage Uп and is limited by the zone of instability of the initial value of the informative parameter of PMT. RFID systems with inductive communication between the identification code carrier and the reader, operate at a frequency below 135 kHz or in the frequency bands 6.78, 13.56, and 27.125 MHz [7, 8].

To increase the reliability of identification in the reader, the procedure of “oscillation” of the frequency of the generated electromagnetic field between the two border values is used. When the frequency of the electromagnetic field exactly coincides with the tuning frequency of the PEOC of the carrier, there is a clear difference in the informative parameter of the PP, which is reliably recorded by the reader. The parameters of the reader and the carrier of the identification code required for reliable identification are regulated by the ISO/IEC 18000 standards [9–11]. Thus ISO/IEC 18000-2:2004, for example, defines:

- The physical level used to communicate between the reader and the identification code carrier.
- Protocol and commands.

- Method of detection and communication with one carrier among several carriers ("anticollision").

The ISO/IEC 18000-2:2004 standard defines two types of carriers: Type A (FDX) and Type B (HDX). These two types differ only in their physical level. Both types support the same interaction protocol. FDX carriers operate at a frequency of 125 kHz and are constantly powered by the reader, including the time of transmission of the identification code from the carrier to the reader. HDX carriers operate at a frequency of 134.2 kHz and receive power from the reader, except for the time of transmission of the identification code from the carrier to the reader. The block diagram of the generalized algorithm of information support of the educational process of the HEI by the ERB identification system is presented in Fig. 3.

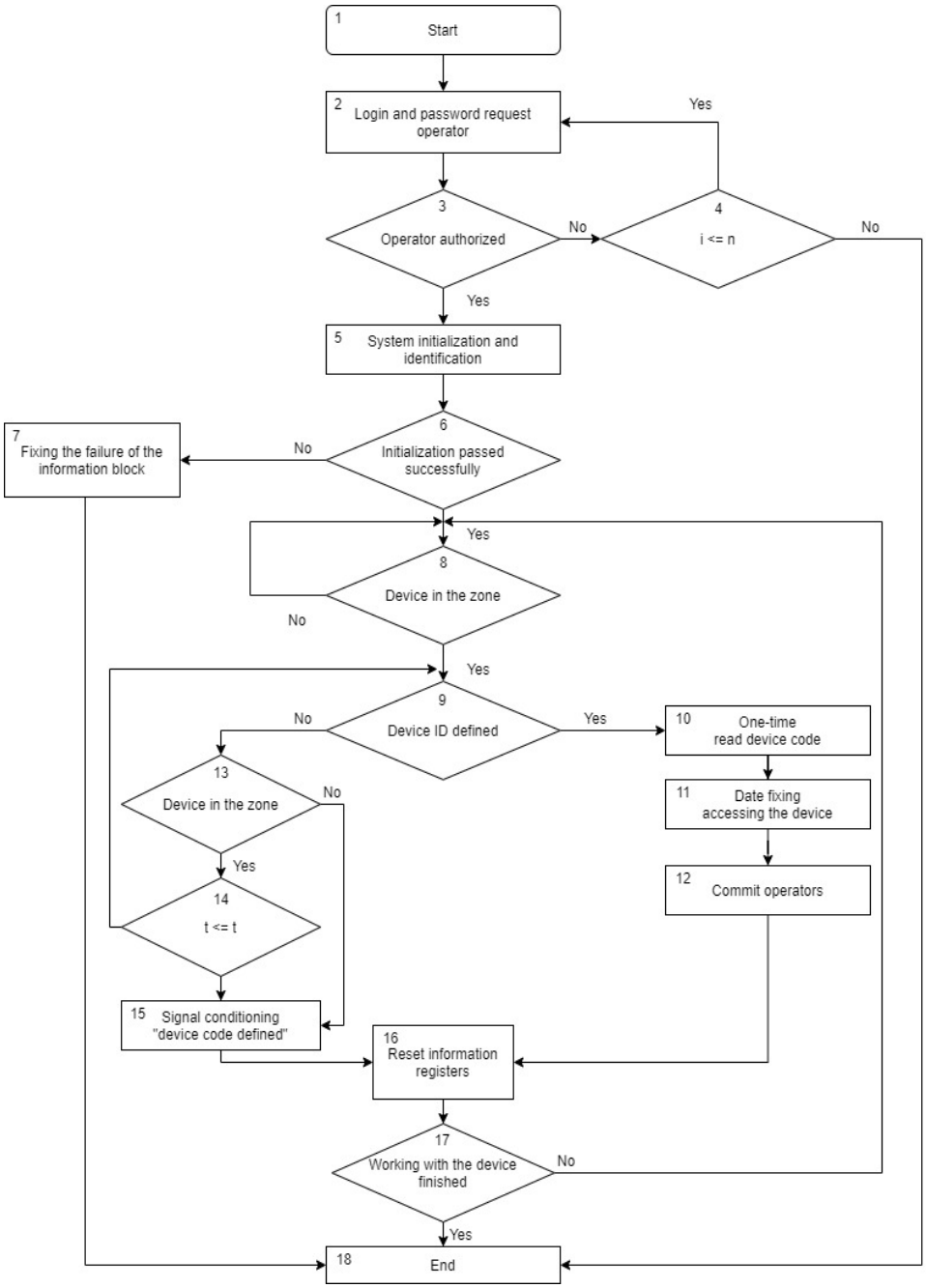

Figure 3: Block diagram of the generalized algorithm of information support of the HEI educational process by the ERB identification system

Initialization of the ERB identification system ensures that the software and hardware of the system are brought into a state of readiness for use. When entering the ERB in the area of identification of the system and the successful code detection, the fixation of this code in the management system of the educational process is carried out (Fig. 1). At the same time, the date of the address to the carrier and the name of the operator are also fixed. After the ERB is removed from the zone, the information registers are reset and the identification system is considered ready to work with the next ERB. In case of failure to determine the ERB code after a certain period, the system generates the signal "carrier code is not defined."

3. Conclusion

In the context of distance learning, i.e. in the absence of direct contact between a teacher and a student due to limited communication channels and means of communication, the creation of an electronic analogue of a paper record book of the applicant for higher education will, as a result, increase the level of academic integrity.

4. References

[1] Law of Ukraine On Higher Education 1556-VII, Bulletin of the Verkhovna Rada 37–38 (2014).

[2] G. M. Gulak, Methodological principles of construction of protected guaranteed information systems of distance learning of higher education institutions, Mathematical Machines and Systems 4 (2020) 136-147.

[3] Law of Ukraine On Electronic Trust Services 2155-VIII, Vedomosti Verkhovnoi Rady 45 (2017).

[4] V. L. Dshkhunyan, V. F. Shangin, Electronic Identification. Contactless Electronic Identifiers and Smart Cards. Moskow, AST Publ., NT Press Publ., 2004. 695 p. [in Russian].

[5] L. V. Kuzmenko, Information technology for creation of perspective guaranteeable automated control systems of objects of critical infrastructure, ITGIP NAS of Ukraine, 2021.

[6] V. K. Zheleznyak, et al., Rationale for the parameters of the measuring transducer in RFID technology with inductive coupling. Vestsi Natsyyanalnai akademii navuk Belarusi. Seryya fizika-technichnych navuk 64 (1) (2019) 98–109, https://doi.org/10.29235/1561-8358-2019-64-1-98-109 [in Russian].

[7] MicroID 125 kHz RFID. System Design Guide, Microchip Technology Inc., 2004. URL: http://ww1.microchip.com/downloads/en/devicedoc/51115f.pdf.

[8] MicroID 13.56 MHz RFID. System Design Guide. Microchip Technology Inc., 2004. URL: http://ww1.microchip.com/downloads/en/devicedoc/21299e.pdf.

[9] ISO/IEC 18000-1:2004. Information technology. Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be standardized. URL: https://www.iso.org/standard/34112.html.

[10] ISO/IEC 18000-2:2009. Information technology. Radio frequency identification for item management. Part 2: Parameters for air interface communications below 135 kHz. URL: https://www.iso.org/standard/46146.html.

[11] ISO/IEC 18000-3:2010. Information technology. Radio frequency identification for item management. Part 3: Parameters for air interface communications at 13,56 MHz. URL: https://www.iso.org/standard/53424.html.