International Journal of Engineering &Technology, 7 (4) (2018) 6494-6499

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.26161
Research paper

Protection of information from unauthorized access in the design of automated systems radionuclide spectrometry for civil engineering

Ilya P. Mikhnev [1, 3] *, Natalia A. Salnikova [1, 3], Svetlana V. Mikhneva [2, 3]

[1] Ph.D in Engineering sciences, Associate Professor, Department of Information Systems and Mathematical Modeling
[2] Ph.D in Juridical sciences, Associate Professor, Department of Theory and History of Law and State
[3] Volgograd Institute of Management - branch of the Russian Presidential Academy of National Economy and Public Administration
**Corresponding author E-mail: mkmco@list.ru*

Abstract

Designing protection systems involves developing a protection model and transferring it to a specific software structure. The security model is a description, formalized or not, of the rules for the interaction of resources in the software-hardware environment of automated systems. Protection models allow you to focus on the most important aspects of the problem of protecting information, discarding the technical details of the system from consideration. The article presents research of information security tools against unauthorized access of automated radionuclide spectrometry systems based on a scintillation gamma spectrometer. As a result of the conducted research, the indicators of the system security were obtained, which allow to calculate and optimize the probability of damage from unauthorized access, taking into account the time of operation and the information security tools used. The developed analytical assessments make it possible at the design stages of automated systems to calculate the upper and lower bounds of the probability of unauthorized access to confidential information.

Keywords: *Civil Engineering; Information Security; Unauthorized Access; Design of Automated Systems; Natural Radionuclides; Radionuclide Spectrometry System.*

1. Introduction

When processing any meaningful information using a separate computer, and even more so in the network, the question arises of how to protect it from unauthorized access and use. The most common method of protection in computer systems is the use of passwords – it is more suitable for protecting access to computing resources than for protecting information. This is a kind of screen that shields legitimate users of the system from outsiders, passing through that, a qualified user gets access to almost all information. At the moment, issues related to the protection of confidential information from unauthorized access in the design of automated systems have become extremely important [1]. In recent years, the construction of buildings used a variety of building materials, both domestic and foreign production. Since the dose loads of indoor exposure depend on the content of activity of natural radionuclide's (NRN) in building materials, the choice of building sites and building designs, it is possible to limit the exposure of the population from natural sources of radiation by interfering with existing construction practices [2], [3].
The existing practice of producing building materials was taking into account their cost. Therefore, consideration of the additional criterion – the degree of radiation impact on the population will lead to a certain increase in the cost of production of building materials [4].

1.1. Relevance of research

For the high accuracy of the estimation of the radiation background in residential premises, an Automated Systems Radionuclide Spectrometry (ASRS) system is required that allows measuring the specific activity of NRN in objects of the external environment, as well as extremely low dose rates of gamma radiation with separation of the contribution to instrument readings due to cosmic and gamma radiation from building materials [5].

1.2. Purpose of work and research tasks

The main goal of this study is to reduce the radon hazard of the building complex and facilities. To do this, you need to solve the following tasks:

1) Identify the patterns and factors of the formation of radiation background caused by radon in the objects of the building complex and premises.
2) To develop methods and means for reducing the activity of radon and daughter products of decomposition (DPD) in the building complex and premises of the Volgograd Region.

2. Automated systems radionuclide spectrometry

To determine the specific activities of NRN in building materials, materials, soil, wood and other, it is advisable to use Automated Systems Radionuclide Spectrometry (ASRS) with an integrated universal spectrometric complex (USC "Gamma Plus R") based

on a scintillation gamma spectrometer, with the software "Progress – 5.1", providing the establishment of a class of material [6]. ASRS "Gamma Plus R" can be used to solve a wide range of radiation monitoring tasks from measurements in the field of certification of the compliance of food products, drinking water, building materials, forestry products, etc. to monitoring and radiation monitoring tasks at nuclear cycle enterprises, and for solving a number of research problems related to the measurement of radioactivity. The unit can be supplied in various configurations in accordance with the customer's requirement. ASRS "Gamma Plus R" consists of detection units, protection from external gamma radiation, an electronic device and an external power supply [7]. But this spectrometer complex does not come with the protection of the software package from malicious code and unauthorized access, which can lead to malfunctions in the PC and loss of information with unauthorized access. Processing spectra, calculation of activity and error is performed using software.

The detection of gamma radiation is based on the recording of effects arising from its interaction with matter. Gamma quanta emitted by atomic nuclei in radioactive transformations have certain physical characteristics that can be used to record them. Measuring the energy and intensity of emitted gamma quanta, and also estimating the half-life of their individual monoenergetic groups, it is possible to identify radionuclides in the measured countable samples and to determine their absolute activity fairly accurately. In order to convert the analog spectrometric signal coming from the detector output, an amplitude-digital converter (ADC) is used in the digital. Managing the work of ADC is carried out using special programs that are part of the software package [8].

Processing of spectra, calculation of activity and errors are performed using the software package "Progress – 5.1". At the present time, the problems of ASRS protection and the critical information infrastructure of the Russian Federation from cyber weapons have sharply escalated, which has made it possible to formulate the relevance of the research that takes place in accordance with the main documents of the RF on security – the National Security Strategy and the Information Security Doctrine of the Russian Federation [9]. According to the Security Council of the Russian Federation, in 2016 more than 50 million cyber attacks on Russian information resources were committed, with 60% of attacks being carried out from abroad [10].

When designing ASRS in the context of the introduction of the digital economy and the development of the global information space, a number of contradictions have arisen, causing the lack of a scientific and methodological apparatus and a uniform methodology for assessing the security of information in the design of ASRS [11], [12]. This is due to:

- Significant uncertainty due to the lack of statistical data on the functioning of a variety of means of information protection (MIP) in the face of growing threats to information security and information and technology attacks;
- The complexity of accounting and formalization of many factors essential for the quantitative evaluation of the security of ASRS (for example, by the variety of information technologies, software, hardware).

At the same time, the need for quantitative assessments of security in connection with the growing number of security threats, as well as the complexity of the objects of analysis, is becoming very relevant.

2.1. Implementation of measures to protect information in the design and operation of ASRS

To ensure the required level of protection of information from unauthorized access in the analysis of radiation characteristics of premises by spectrometric method, as well as the design and operation of automated radionuclide spectrometry systems, organizational, technical and organizational and technical measures for protecting information are implemented [13], [14].

Organizational measures are intended for managers, information protection bodies, other users and are the organization, streamlining, monitoring of activities to protect information in the organization. Technical and organizational and technical measures to protect information include the use of technical means, which are combined into information protection systems (IPS) and are an integral part of ASRS [15].

The degree of implementation of measures to protect information is assessed in the design and operation of ASRS and depends on the optimal acquisition of the IPS by means of information protection (MIP) and the performance of the IPS as a whole [16].

It is known that the intruder will always spend the time T_{UAA} necessary to create a channel for the implementation of the information security threat to the implementation of unauthorized access (UAA) to information resulting in the disruption of the normal functioning of automated radionuclide spectrometry systems, confidentiality, integrity and accessibility of information, time characterizes the time interval:

$$T_{UAA} = \sum_{i=1}^{4} T_i \quad (1)$$

Where T_1 - identify the vulnerabilities of software (hardware); T_2 - assessment of the possibility of exploiting the vulnerability, taking into account the existing information protection system of the proposed impact object (information carrier); T_3 - the choice of how to implement the UAA; T_4 - implementation of the UAA.

On this basis, by increasing T_i, it would always be possible to control the security of information in ASRS. That is, T_i could be adopted as a criterion for evaluating the security of information in ASRS. Then, by setting the threshold value $T_{add.\,UAA}$ in the design of ASRS and ensuring the condition $T_{UAA} \leq T_{add.\,UAA}$, it is possible to implement the permissible protection of restricted access information in ASRS [17], [18].

However, such an approach will not reflect the real picture, since the time Ti is a random variable whose distribution law is difficult to compute, since it will vary depending on the capabilities of the offender. In addition, it does not take into account the main factors of exploitation, such as: various threats to information security in ASRS, ASRS operational time, characteristics of the means of information protection (MIP) used, on which also unauthorized access to information [19].

Therefore, to improve the objectivity of monitoring the timeliness, reliability, completeness and continuity of information security designed by ASRS, it is advisable to develop a mathematical model of the probability of unauthorized access to circulating information, taking into account the operating conditions and the composition of the information protection system (IPS). Based on the found model, to formulate qualitative and quantitative criteria for increasing the security of information in the design of ASRS [20].

It is known that the classical formulation of the task of developing a set of information security tools to ensure maximum performance of ASRS in the conditions of UAA will look like:

$U_\Sigma \rightarrow \min,$

$$C = C_{opt} \quad (2)$$

Where U_Σ is the total damage caused; C – the costs of designing a complex of information security tools; or

$E_3 \rightarrow \max, \delta_3 \rightarrow \max,$

$$C = C_{opt}\ C = C_{opt} \quad (3)$$

Where E_3 is the performance of the ASRS; δ_3 – relative efficiency of ASRS functioning.

Despite the apparent simplicity of the classical formulation of the problem, in practice it is rarely possible to use the results given. This is explained by the complexity of the mathematical descrip-

tion of the reduction of possible UAA from the costs of designing the IPS. If the dependence of security on the cost of protection can be obtained by having the technical and cost characteristics of the available remedies on the market, it is extremely difficult to estimate the actual damage from the UAA, since this damage also depends on a variety of factors affecting the probability of damage. For example, the damage will depend on: the number of units included in the ASRS, the characteristics of the MIP, the number of possible security threats in ASRS, the qualification of the offender and the number of attempts to implement security threats, the consequences of unauthorized access, etc.

At the same time, the design of the IPS for ASRS critical information infrastructure, for example, related to the management of nuclear power plants for which the UAA to information resources can lead to disastrous consequences, the selection of the MIP is carried out with the best indicators, and therefore, the effect of the cost of protection on efficiency can be neglected, that is,

If

C << U, then:

$$U_{\Sigma} = \frac{U}{f(C)} \tag{4}$$

In this case, (2) and (3) take the form:

$U_{\Sigma} \rightarrow \min$,

$$C \le C_{add} \tag{5}$$

Or

$E_3 \rightarrow \max$, $\delta_3 \rightarrow \max$,

$$C \le C_{add}\ C \le C_{add} \tag{6}$$

Where C_{add} – the allowable costs of protection.

Thus, the UAA to information in ASRS will depend on the applied MIP, on the number of threats to information security, the degree of security and the time of operation of the ASRS. In accordance with GOST R 50922-2006 "Information security. Basic terms and definitions" the purpose of information protection is to prevent damage to the owner of information in connection with possible misinformation to information, violation of the normal functioning of ASRS, theft, modification or destruction of information [21].

Obviously, the maximum damage can be inflicted when the information in the ASRS is compromised completely. Such a situation may arise under the following conditions: either when the ASRS is captured by the enemy, or in the situation when the total information and technical attacks of the enemy allow him to provide the UAA to the protected information circulating through all the protected ASRS channels [22]. If one security threat is realized, then in modeling we will assume that this leads to minimal damage. Let us formulate the problem and find an expression for the probability of the UAA to the information circulating in the ASRS. Let ASRS be projected, containing k units, in each of which it is possible to implement N_i, i = 1, 2 ... k threats to information security. In total, ASRS contains S possible to implement security threats, and

$$S = N_1 + N_2 + ... + N_k = \sum_{i=1}^{k} N_i \tag{7}$$

Parrying security threats is carried out by MIP, included in the IPS. MIP have different functionality to provide protection, depending on the characteristics, protection mechanisms being implemented, technical requirements, compatibility with other protection measures, economic and ergonomic characteristics. To distinguish the complex of information protection systems (IPS), it is advisable to introduce the weight coefficients M_i, i = 1, 2 … k. The higher the degree of secrecy of the information being processed, the stricter the protection requirements and the higher the technical requirements, the higher the value should be assigned to the coefficient M_i and vice versa. Suppose that possible unauthorized access to information when implementing at least one security risk occurs with probability P_x, and the probability of unauthorized access to information in the implementation of all security threats P_y.

Recall that the Automated Systems Radionuclide Spectrometry under consideration contains S possible security threats. Suppose that all threats are random with an equiprobable distribution law. Then, the probability of UAA to information when implementing one specific security threat without a relative place of its implementation and IPS protection from the UAA is defined as:

$$P_s = \frac{1}{S} \tag{8}$$

In order to take into account, the vulnerabilities of the ASRS unit, the availability of which is a prerequisite for the formation of a security risk channel, it is necessary to introduce in the formula (8) a weighting coefficient M_i taking into account the characteristics of the used information protection tools for this i-th unit. If M_i is introduced into the denominator of expression (8), the resulting expression will reflect the physics of the UAA process to information in the implementation of one threat to the security of the i-th unit, i.e. we obtain:

$$P_{iS} = \frac{1}{M_i + S} \tag{9}$$

Indeed, if $M_i = 0$, which corresponds to the lack of protection, then (9) turns into (8). And if M_i increases, then the probability of an unauthorized access to information will decrease, which correctly reflects the physics of the phenomenon. There are various methods for determining the exact quantitative estimate of M_i, for example, with the help of expert assessments described and implemented in the works of T. Saati, M. Eddous, R. Stansfield, O.I. Laricheva, V.B. Korobov. The common property of all methods is the ability to vary the values in the required limits for the problem, for example, within the range of 1 to 10 or within the limits of large values. This "weighing" of the MIP with the help of the M_i coefficient allows us to correctly reflect the qualitative picture of the UAA process to the information and, consequently, will allow (9) to work out the quality recommendations.

Recall that ASRS of an arbitrary i-th unit contains possible security threats for implementation. Therefore, for the UAA probability to information U_i, if at least one security threat from N_i possible threats of the i-th subdivision is realized, the following will be true:

$$U_i = 1 - (1 - P_{iS})^{N_i} \tag{10}$$

Similar types of security threats exist in k units, where they can also form channels for the implementation of threats. Therefore, for the probability UAA to information when implementing at least one security threat, taking into account all k units, the expression determined by the formula for calculating the total probability of events will be valid:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \sum_{i=1}^{k} \frac{N_i}{S} \left[1 - (1 - P_{iS})^{N_i}\right] \tag{11}$$

Where the value of η_i is determined by the relation:

$$\eta_i = \frac{N_i}{S} \tag{12}$$

The value of P_x indicates the probability of UAA to information in at least one department when implementing at least one security

threat, that is, the probability of UAA to information when implementing at least one of the S threats. In the event that the units have the same number of possible security threats, i.e.

$$N_1 = N_2 = ... = N_k \ , \ S = N_1 + N_2 + ... + N_k = k \cdot N_i \quad (13)$$

Consequently

$$\eta_i = \frac{N_i}{S} = \frac{N_i}{k \cdot N_i} = \frac{1}{k} \ , \quad (14)$$

Then formula (11) takes the following form:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \frac{1}{k} \sum_{i=1}^{k} \left[1 - (1 - P_{iS})^{N_i} \right] \quad (15)$$

Note that formula (11 and 15) determines the UAA probability of information when implementing at least one of the possible security threats for all units in ASRS. It is fair to assume that in this case the total damage caused will be minimally possible. On the other hand, the probability of UAA to information when implementing at least one security threat as a security feature will take the maximum possible value, i.e. the upper bound on the probability of UAA for information in ASRS.

Next, we introduce the following assessment of the security of information, defined as the probability of UAA to information when all possible security threats are realized simultaneously. The maximum damage occurs when, as mentioned above, when implementing all possible security threats, that is:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i} \quad (16)$$

Thus, two estimates of ASRS P_x and P_y security are given and give the upper and lower bounds of the UAA probability to information, which corresponds to the best and worst case of damage to ASRS as a whole. Nevertheless, it is obvious that expressions (11) and (16) are valid only for one attempt to implement a security threat. Theoretically, during the lifetime of the ASRS, such attempts can be innumerable. It is almost impossible to quantify the number of attempts to implement security threats. However, it is possible to set a step a priori of these attempts in time. At the same time, during which one attempt to implement a security threat (T_p) can be set taking into account the actual conditions of exploitation and the socio-political, military situation.

For example, the step of realizing the security threat in peacetime can be equated to one month, a week, and during the fighting several days, 24 hours, etc. For a given value of the T_p interval, it is possible to determine the number of possible attempts to implement security threats R during the ASRS operation of the object T:

$$R = \frac{T}{T_p} \ , \quad (17)$$

Where T is the operating time, and T_p is the step of implementing the security threat.

Knowing the number of attempts, it is possible to estimate the probability of UAA to protected information when implementing all or at least one security risk during the operation T:

$$P(t) = 1 - (1 - P_k)^R \ , \quad (18)$$

Where the value of P_k is some estimate that characterizes the probability of one successful attempt to implement a security threat, and t = T. We note that previously we gave two methods for calculating the estimates of P_k: P_x and P_y for the best and worst cases, respectively. Therefore, if it is necessary to calculate the probability that the UAA will be implemented to the information for a period of time T when implementing at least one security threats (ST), the value $P_k = P_x$ must be substituted into expression (13). On the other hand, it is necessary to calculate the probability of the worst case for the system, that is, the UAA in the implementation of all possible ST ASRS simultaneously. Then, in the expression (18), the value P_y must be substituted for P_k.

It should be emphasized that expression (18) can be used both for the entire ST list for a particular ASRS, and selectively for threats that make up a certain direction. In particular, we can distinguish ST, in the implementation of which the confidentiality of information, its integrity or accessibility is violated. For different ASRS, the damage from the implementation of ST of different directions may be significantly different. This is due to the variety of ASRS for the functions performed. For example, threats to confidentiality of information for ASRS are of an informational nature more urgent than threats aimed at breaching the availability of information. On the other hand, for ASRS management of a critical object, threats of breach of availability and integrity of information play a major role, due to possible consequences due to a malfunction of the system. Such polymorphism of expression (18) is its important advantage, since there is no need to correct methods of calculating the information security rating depending on the composition of ST in ASRS.

3. The obtained quantitative results of simulation modeling

The obtained quantitative results of simulation can be presented in tabular or graphical form. It should be emphasized that expression (18) gives an upper bound for the UAA probability to information in ASRS, that is, for the worst case, which is a particularly important indicator in the design of ASRS.

In Table 1 shows how the security estimates P_x and P_y for ASRS with different initial parameters are numerically different. In Table 2 shows the UAA probability of information for the implementation of at least one ST and for the implementation of all STs simultaneously, taking into account the number of ST implementation attempts for ASRS 4 and ASRS 7 from Table 1.

Let's analyze the dependence of the quantitative estimation of the UAA probability on information when at least one ST P_x is realized from the operation parameters of ASRS. So in the table 1 the largest value $P_x = 0.265$ takes in ASRS No. 5 when the number of ST S = 40. At smaller values of S, the value of P_x will decrease: $P_x = 0.232$ when the number of S = 20 in ASRS No. 3, $P_x = 0.251$ when the number of S = 30 in ASRS No. 4, $P_x = 0.251$ with the number S = 12 in ASRS No. 1, $P_x = 0.248$ with the number S = 15 in ASRS No. 2.

Table 1: Evaluation of Information Security for Automated Systems of Radionuclide Spectrometry

	ASRS 1	ASRS 2	ASRS 3	ASRS 4	ASRS 5	ASRS 6	ASRS 7
S	12	15	20	30	40	50	50
K	3	3	3	3	3	4	4
N_1	3	5	5	4	10	10	10
N_2	4	5	6	6	10	10	10
N_3	5	5	7	10	10	10	10
M_1	3	3	9	5	3	6	4
M_2	4	3	3	2	3	6	5
M_3	2	3	6	9	3	6	9
P_1	0.066	0.055	0.037	0.040	0.030	0.021	0.022
P_2	0.063	0.055	0.047	0.045	0.030	0.021	0.023
P_3	0.071	0.055	0.042	0.034	0.030	0.021	0.020
U_1	0.187	0.248	0.172	0.151	0.265	0.197	0.205
U_2	0.227	0.248	0.254	0.243	0.265	0.197	0.209
U_3	0.309	0.248	0.257	0.296	0.265	0.197	0.186
P_x	0.251	0.248	0.232	0.251	0.265	0.197	0.198
P_y	8.41E-15	1.48E-19	1.77E-25	5.37E-29	2.78E-46	3.09E-67	3.28E-67

It is established that the smallest value $P_x = 0.232$ takes in ASRS No. 3, where the IPS weighting by subdivision has the largest

values (9, 3, 6). In other ASRS, with smaller weighting coefficients IPS, the value of P_x is smaller.

Table 2: Assessment of the Security of Information in ASRS, Depending on the Number of Possible Attempts to Implement Security Threats

Number of attempts R	ASRS 4		ASRS 7	
	P_x	P_y	P_x	P_y
0.20	0.056	3.29E-34	0.048	6.36E-73
0.25	0.069	8.25E-32	0.059	4.74E-70
0.33	0.092	1.26E-32	0.079	7.58E-69
0.5	0.134	5.48E-30	0.116	4.67E-67
1	0.251	5.37E-29	0.218	3.08E-65
2	0.439	7.29E-27	0.389	2.45E-62
3	0.580	2.64E-25	0.523	6.37E-60
4	0.685	1.25E-24	0.627	4.25E-57
5	0.764	9.83E-21	0.709	7.67E-53
6	0.823	5.37E-20	0.772	2.92E-51

It should be noted that in the case when the weights of the IPS are uniform in all divisions of one ASRS, the probability of implementing at least one ST is lower than in another ASRS with divisions having different weights of IPS. And the total weighting coefficient of IPS of all divisions of both ASRS is the same. So in ASRS No. 6 and ASRS No. 7, an equal number of S = 50, the same number of divisions K = 4 and the same distribution of ST between divisions - 10 ST in each K. However, the weights of IPS by division are different: ASRS No. 6 (6, 6, 6), ASRS No. 7 (4, 5, 9). The total weighting factor in both ASRS is 18. At the same time, $P_x = 0.197$ for automated system of radionuclide spectrometry No. 6 is less than, $P_x = 0.198$ for automated system of radionuclide spectrometry No. 7.

4. Practical value and work conclusion

After analyzing the table 2, we can conclude that P_x significantly increases with the growth of attempts to implement security threats. So for ASRS No. 4 P_x at one attempt is equal to 0.251. When the offender makes five attempts, this probability will reach a value of 0.764. Thus, the developed analytical estimations allow at the ASRS design stages to calculate the upper and lower bounds of the UAA probability for information, which is extremely important for the ASRS design. As it enables to optimize the probability of damage in relation to the operation time, the number of security threats, the applied information security tools, the given information security class, and the number of attempts to implement security threats.

References

[1] Kamaev VA, Mikhnev IP & Salnikova NA, "Natural Radionuclides as a Source of Background Irradiation Affecting People Inside Buildings", Procedia Engineering, vol. 150, (2016), pp. 1663-1672. https://doi.org/10.1016/j.proeng.2016.07.148.

[2] Mikhnev IP, Salnikova NA & Lempert MB, "Research of Activity of Natural Radionuclides in Construction Raw Materials of the Volgograd Region", Solid State Phenomena, vol. 265, (2017), pp. 27-32. https://doi.org/10.4028/www.scientific.net/SSP.265.27.

[3] Kravets AG, Salnikova NA, Lempert LB, Mikhnev IP & Mikhneva SV, "Modern Management Technologies of the Department for Providing Epidemiological Supervision of the Volgograd Region", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8, Issue-6S, (2019), pp. 453-458. https://www.ijitee.org/download/volume-8-issue-6S.

[4] Orudjev NY, Lempert MB, Osaulenko I, Salnikova NA, Kuzmichev AA & Kravets AG, "Computer - Based Visual Analysis of Ecology Influence on Human Mental Health", In Proceedings of the 7th International Conference on Information, Intelligence, Systems and Applications (IISA 2016), (2016), pp. 1-6. https://doi.org/10.1109/IISA.2016.7785416.

[5] Mikhnev IP, Salnikova NA & Lempert MB, "Modern Condition of Dose Loads from Construction Materials and Main Sources of Ionizing Impact on the Population of the Volgograd Region", Materials Science Forum, vol. 931, (2018), pp. 1007-1012. https://doi.org/10.4028/www.scientific.net/MSF.931.1007.

[6] Mikhnev IP, Mikhneva SV & Salnikova NA, "Studies of radon activity in civil engineering and environmental objects", International Journal of Engineering & Technology, [S.l.], vol. 7, No.2.23, (2018), pp. 162-166. https://doi.org/10.14419/ijet.v7i2.23.11907.

[7] Kamaev VA, Fomenkov SA & Davidov DA, "Use of physical knowledge for automation of the initial stages of designing, Proceedings", International Conference on Artificial Intelligence Systems (ICAIS 2002), IEEE, (2002), pp. 411 – 413.

[8] The Doctrine of Information Security of the Russian Federation (approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646), Collection of Legislation of the Russian Federation, 12.12.2016, No. 50, art. 7074, 2016.

[9] Russian newspaper, 15.02.2017 Security Council: The number of cyber-attacks on the Russian Federation in 2016 has tripled, [Electronic resource], Access mode: https://rg.ru/2017/02/15/sovbez-chislo-kiberatak-na-rf-za-2016-god-vyroslo-vtroe.html (date of circulation: 30.09.2018).

[10] Mikhnev IP, Salnikova NA & Mikhneva SV, "Effect of Thermal Treatment of Building Materials on Natural Radionuclides Effective Specific Activity", Materials Science Forum, vol. 945, (2019), pp. 30-35. https://doi.org/10.4028/www.scientific.net/MSF.945.30.

[11] Kravets A & Kozunova S, "The risk management model of design department's PDM information system", Communications in Computer and Information Science (CCIS-2017), vol. 754, (2017), pp. 490-500. https://doi.org/10.1007/978-3-319-65551-2_36.

[12] Mikhnev IP, Salnikova NA & Mikhneva SV, "New Industrial Technologies and Innovations for the Production of Nanostructured Materials", Advances in Social Science, Education and Humanities Research, vol. 240, (2019), pp. 83-89. https://doi.org/10.2991/sicni-18.2019.18.

[13] Salnikova NA, Lempert BA & Lempert MB, "Integration of Methods to Quantify the Quality of Medical Care in the Automated Processing Systems of Medical and Economic Information", Communications in Computer and Information Science (CCIS), vol. 535, Springer, Volgograd; Russia Federation, (2015), pp. 307-319. https://doi.org/10.1007/978-3-319-23766-4_25.

[14] Orudjev NY, Poplavskaya OV, Lempert LB & Salnikova NA, "Problems of Medical Confidentiality While Using Electronic Documents in Psychiatric Practice", Atlantis Press, Proceedings of the 2016 conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM), vol.51, (2016), pp. 120-125. https://doi.org/10.2991/itsmssm-16.2016.75.

[15] Shcherbakov M, Groumpos PP & Kravets A, "A method and IR4I index indicating the readiness of business processes for data science solutions", Communications in Computer and Information Science (CCIS-2017), vol. 754, (2017), pp. 21-34,. https://doi.org/10.1007/978-3-319-65551-2_2.

[16] Mikhnev IP, Salnikova NA, Lempert MB & Dmitrenko KYu, "The Biological Effects of Natural Radionuclides from the Construction Materials on the Population of the Volgograd Region", 8th International Conference on Information, Intelligence, Systems and Applications (IISA-2017), IEEE, (2017), pp.1-6. https://doi.org/10.1109/IISA.2017.8316428.

[17] Dyachenko T, Ivanenko V, Lempert B & Salnikova N, "Dynamics of Health Care Quality Indicators at Inpatient Hospitals of the Volgograd Region Estimated by an Automated Information System", Communications in Computer and Information Science (CIT&DS-2017), vol. 754, Springer, Volgograd, Russia, (2017), pp. 847-857. https://doi.org/10.1007/978-3-319-65551-2_61.

[18] Golubev AV, Shcherbakov MV, Scherbakova NL & Kamaev VA, "Automatic multi-steps forecasting method for multi seasonal time series based on symbolic aggregate approximation and grid search approaches", Journal of Fundamental and Applied Sciences, vol. 8, No. 3S, (2016), pp. 2429-2441.

[19] Korotkov A, Kravets AG, Voronin YF & Kravets AD, "Simulation of the initial stages of software development", International Journal of Applied Engineering Research, vol. 9 (22), (2014), pp. 16957-16964.

[20] GOST R 50922-2006, National standard of the Russian Federation, Data protection, Basic terms and definitions, Moscow, Standartinform, 2008.

[21] Mikhnev IP, Salnikova NA & Mikhneva SV, "Digital technologies for searching and processing unstructured Information in modern higher education", Advances in Economics, Business and Management Research, vol. 81, (2019), pp. 620-625. https://doi.org/10.2991/mtde-19.2019.124.

[22] Kravets A, Poplavskaya O, Lempert L, Salnikova N & Medintseva I, "The Development of Medical Diagnostics Module for

Psychotherapeutic Practice", Communications in Computer and Information Science (CIT&DS-2017), vol. 754, Springer, Volgograd, Russia, (2017), pp. 872-883. https://doi.org/10.1007/978-3-319-65551-2_63.