Information Security Specialist Readiness Indicator as a Part of the Trusted Digital Environment

Anastasiya Arkhipova [1]

[1] *Novosibirsk State Technical University, 20 Prospekt K. Marksa, Novosibirsk, 630073, Russia*

Abstract

The article discusses the role of monitoring, comprehensive, systematic audit of the current state of the organization's resources and infrastructure. The hypothesis of the influence of the human factor within the risks of information security of the enterprise from personnel is highlighted. The article presents the technology of formation of qualitative and quantitative indicators in the form of the information security specialist readiness as an element of a trusted environment figure. Tools of readiness indicator formation within the framework of specialists training, as well as within the framework of players with elements of introduction in social engineering, are considered. The proposed article fills the lacks in the theoretical and methodological basis of readiness indicators for technical specialties using complex equipment as objects of study. Also highlighted are the main indicators of the educational component (readiness indicator) of an information security specialist. The evolution of category is presented, the basic requirements, criteria, and indicators of estimation of readiness indicator. The article proposes also a simulation model of the functioning of the Federal E-Employment operator FO and Regional e-employment operator (RO) in the modern labor market based on the Petri network. Experiments have shown that the use of readiness indicators has a positive impact on the quality of education in the trusted digital environment in the field of information security.

Keywords 1

information security, cybersecurity, security level, security audit, readiness indicator, social engineering, cyber gaming, education, model, the human factor

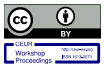
1. Introduction

The issues of vulnerabilities in corporate systems, access to information of critical infrastructure objects are some of the central issues of information security today. According to the analytics of leading companies in the field of information security, the number of large-scale attacks at the level of organizations regardless of type (government, private companies, service providers, etc.) increases annually. The growth's stimulant, in this case, is both the growth of the position of the number of connected equipment on the Internet and the transition of companies in the context of the digital formation of States according to some stages from an initial electronic government to an open government, further to a datacentric government with the ultimate goal of moving to the stage of "smart government". This trend will exponentially contribute to the further increase in information security risks. From these positions, the need for monitoring and comprehensive, systematic audit of the current state of resources and infrastructure of organizations is taking a serious turn [9].

According to statistics of conducted audits of information security, the central problem of the security of the organization is the problem of the influence of the human factor. Indeed, risks from

Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea

EMAIL: arhipova_ab@mail.com (A. 1)
ORCID: 0000-0003-0791-8087 (A. 1)



© 2021 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3057/paper4.pdf

personnel represent a distinct group of information security risks of the organization with a specific set of causes and conditions for their implementation.

Today, in the framework of employment, applicants are not only required to comply with the professional model of the specialist in the context of professional skills (hard skills), but also a certain complex of psychophysiological characteristics (soft skills). Thus, the optimal combination of soft skills and hard skills presents some models of a graduate of an educational institution to the context of a continuous education model [7]. This article attempts to focus on the field of information security [3, 12]. However, it can be extended to other spectra and interdisciplinary areas of research.

The purpose of this article is to describe the technology of generating the readiness indicator of an information security specialist as an element of a trusted digital environment.

2. The Essence of Specialist Readiness Indicator

Historically, the problem of the specialist's readiness for professional activities was central in the development of national economic sectors. And if in modern reality they emphasize from the position of the conceptual apparatus «readiness», then some time ago the emphasis shifted to the concepts of «factor», «human factor».

After analyzing the conceptual apparatus, we can conclude that the correlation of the categories under consideration is more than high. Even S. A. Kuznetsov in the Great Interpretive Dictionary of the Russian language considers the factor in the form of «significant circumstance contributing to the process or phenomenon», the human factor in the form of «the role and significance of a person in public life, social processes with a person as a subject of activity», readiness as a certain inclination, and in a combination of «professional readiness» sees as a tendency related to professionalism [7, 8].

With the growth of production and the development of the national economy sectors, the increase in knowledge-intensive production, the center for the study of categories shifted and became an application of the different spheres. Thus, readiness was considered from the standpoint of a combination of factors, such as scientific knowledge, the organizational structure of the enterprise with a set of internal and external relations, moral and social qualities [3, 11]. And the complexity of these factors represented the human factor.

On the other hand, it is possible to represent that the human factor as a specific individual contribution to the formation of quality and system effectiveness issues in which it has been in operation. Thus, we can conclude a combination of the number of internal (natural) and external (social) elements. Then a comprehensive assessment of the influence of the human factor on the subject area (for example, information security) as part of the assessment of the specialist readiness indicator is possible from the position of the combination of soft skills and hard skills, which are the results of the characteristics vector:

- energy, characterizing the level of physiologically functions activity and systems (circulation, respiration, etc.);
- information characterizing processing of received information and making decisions based on it, i.e. reflecting cognitive processes (thinking, memory, motivation, personality structure, individuality);
- effector, responsible for the implementation of the adopted decisions (quantitative and qualitative indicators of professional activity and physiological parameters);
- activation, which determines the orientation and degree of tension of professional activity: level of attention, stress resistance, peculiarities of the motivational sphere [7].

The modern concept of the human factor is not limited to the analysis of knowledge embodied in the person and contributing to creative work, demonstrating a broader approach, considering as human potential not only knowledge embodied in a person but also accumulated scientific knowledge objectified in new databases, etc., as well as relations with other economic entities.

The human factor can be defined as a specific human contribution to the quality and effectiveness of the various systems of which it is an element [11] (Table 1).

Thus, the human factor, on the one hand, is a component of the system, on the other hand, is itself a system category, forming a plurality of system constructions in which it acts as a subsystem or element thereof.

Table 1
Human factor as a system category

System attribute	Implementation in the human factor.
Structural properties	A human factor is a complex event.
Integration	A human factor is developing on the interaction of environment (economics, politics, physics, etc.).
Detached process properties	A human factor is a local element in the common set.
Hierarchical properties	A human factor is a multidimensional concept consisting of a large number of structural invariants reflecting different sides and properties of the human factor as a system.
Not additivity properties	Infeasibility of human factor's properties to the total of its constituent components, if the system has integrative qualities.

The human factor includes both natural and social elements, many of which can be developed and improved through physical and psychological actions, education. Forming and accumulating during the life of an individual, the human factor as the production develops loses the signs of a natural resource, acquiring the features of the formed and reproduced. The main element here is continuing education, which contributes to the formation of the social component of the human factor.

Note that the list of the composite human factor is not exhaustive, since it can be supplemented or modified. For example, it is permissible to split the social potential of the human factor into information security.

According to statistics of conducted information security audits, the central problem of security in different organizations is the influence of the human factor [1]. Indeed, risks from personnel constitute the separate group of information security risks of the organization with the specific sets of causes and conditions for their implementation. Therefore, the issue of quality training according to the current requirements and demands of the modern labor market is more than a priority in the context of a trusted digital environment at the open state stage of the country.

Today, in the framework of employment, applicants are required not only to comply with the competent model of a specialist in the context of professional skills (hard skills), but also a certain complex of psychophysiological characteristics (soft skills). Thus, the optimal combination of soft skills and hard skills represents some model of an abstract graduating student of an educational institution to the context of a continuous education model [7]. This article attempts to focus on the field of information security as the author's immediate subject area [3, 11]. However, it can be extended to other spectrum and interdisciplinary areas of research.

The purpose of this article is to describe the technology of generating information security specialist readiness indicators as part of the trusted digital environment.

3. The Technology of Specialist Readiness Indicator Generation

The specialist readiness indicator is directly related to the subject area, therefore, the specialist readiness technology is logical to build from these positions. Let's take a look at information security. The effective solution of problems in this area requires highly organized, highly qualified personnel support, ranging from the employment procedure to continuous processes of advanced training, retraining taking into account program and technological, organizational changes in the information security of the open state. Moreover, the procedure of employing a specialist from the position of a readiness indicator involves an analysis of its characteristics, while the working process is accompanied by the effect of accumulative frequencies of the factors included in it, as well as the formation of additional links [14].

According to the Law on Education, "the education system creates conditions for continuing education through the implementation of basic educational programs and various additional educational programs, the provision of the opportunity to simultaneously master several educational programs, as well as taking into account the available education, qualifications, practical experience in obtaining education". In the context of continuing education, we will formulate the main stages of the development of the indicator of readiness of information security specialists (Figure 1).

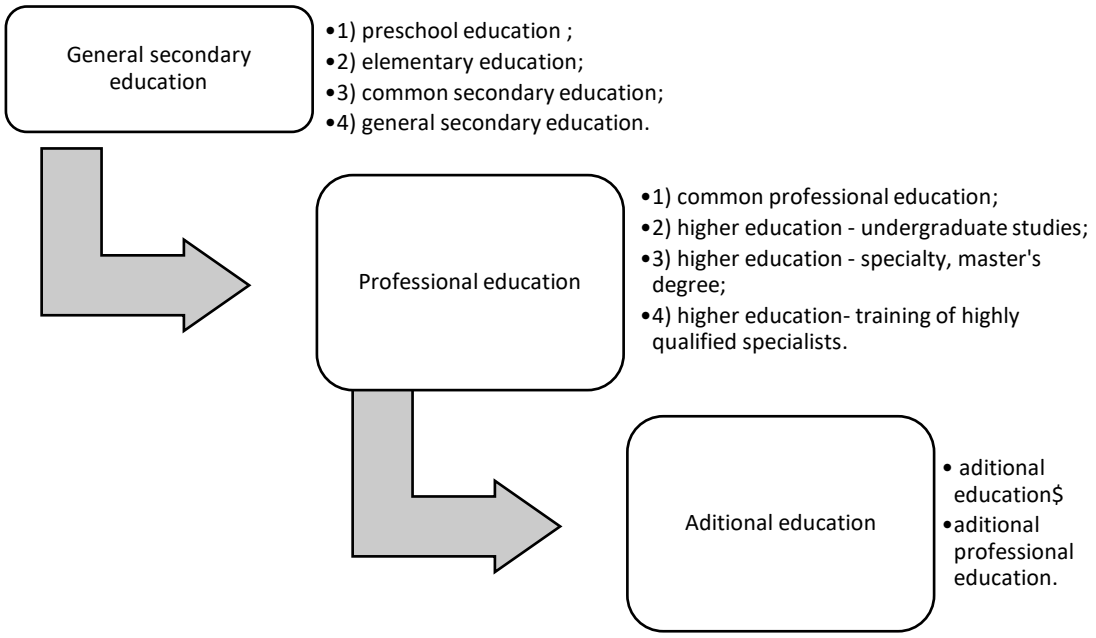


Figure 1: Education levels in the Russian Federation

Therefore, to generate a readiness index, it is necessary to enter a group of cumulative factors for the assessment of soft skills and hard skills, as well as nominal characteristics with branching by categories and types/forms of education.

Within the project supported by Charity Foundation of Potanin in 2021 in FGBOOU WAUGH "Novosibirsk State Technical University" is developed in the scientific purposes the automated system of assessment of an indicator of readiness of experts of the direction 10.03.01 "Information security" and 10.05.03 "Information security of the automated systems". This system is a tool for monitoring and analyzing training results. The impact of gamblers in the implementation of programs for the education of an enlarged group of specialties 10.00.00 "Information Security" [7, 12] is also evaluated.

Implementation of the automated system for the readiness indicator modeling can be one of the useful methods. Algorithm or the comprehensive approach to the estimation of specialists readiness, based on the results of the expert questioning, accumulated frequencies (fuzzy model with linguistic and point scales). It consists of the next blocks:

To create and operate the above-mentioned system, a generalized algorithm for estimating the readiness indicator is implemented as the result of the following units:

Block 1. Modeling the definition of readiness indicator.

Block 2. Generation of readiness indicators benchmarks.

Block 3. Procedure for assessment of readiness indicator.

Block 4. Generalization and interpretation of the results.

Block 5. Forming of conclusions and adjustment of model.

Block 1 is one of the most complexes since it involves the analysis and formalization of criteria and the selection of readiness indicator indicators. Every indicator contains both quantitative and qualitative indicators. Quantitative indicators include specialty/direction data resulting from the competency model in the section of the blocks of disciplines of the curriculum. Qualitative indicators represent a complex of psychophysiological characteristics within the framework of the given direction. Quantitative criteria for choosing indicators should be valid, effective, systemic, and measurable (the quantitative and quality aspects).

The technology for generating the specialist readiness indicator is presented in the form of a multi-level structure and involves a consistent solution at all stages: **stage 1, stage 2, stage 3**.

Stage 1 is time-consuming because it requires the collection and processing of information. By the indicator of readiness of a graduate at this stage is understood: the level of educational achievements of a graduate of an educational institution; an indicator of psychological indicators; the level of interest of the graduate in the field of information security.

1. The level of readiness of a student to study at a university (P_{01}^1) is an expression of the following form:

$$P_{01}^1 = \sum_{j=1}^{n} k_j \cdot \left(\sum_{i=1}^{m_j} \left(D_{X_{ij}} \cdot \alpha \quad \cdot (1 - \omega_i) + \omega_i \cdot (1 - \alpha \quad) \cdot P_{X_{ij}} \right) \right), \tag{1}$$

where где j – the result of curriculum training ($1<j\leq n$, n – disciplines curriculum); k_j - coefficient of the significance of disciplines j ($0 < k_j < 1$); $D_{X_{ij}}$- total result X_i by discipline j ($25 \leq D_{X_{ij}} \leq 100$); α – summary coefficient of significance ($0 < \alpha < 1$); weight w_i={0, 1}, $P_{X_{ij}}$- total graduated result X_i of discipline j ($25 \leq P_{X_{ij}} \leq 100$); m_j – number of disciplines in curriculum training part j.

2. The indicator of psychological suitability (P_{01}^2) is a complex three-component qualitative indicator that combines data on the attention, accuracy of a graduate when working with service documentation, etc. Evaluation is carried out on 5 levels: A - high, B - above average, C - medium, D - below average, E - low.

3. The level of interest in the field of information security (P_{01}^3,%) is an assessment of the level of interest of a graduate of an educational institution based on comprehensive methods.

Stage 2 includes the professional selection of applicants based on the set of obtained indicators.

Stage 3 involves the formation of a readiness indicator based on the entire period of study at the university. The indicator takes into account the set of nominal and calculated characteristics.

An integral evaluation in a theoretical and practical context is a weighted average estimate. As weights, we take the normalized coefficient of significance, calculated as the results of an expert survey:

$$L_t = \alpha \sum_{j=1}^{n} PN_{Cj} \cdot \sum_{i=1}^{k} dt_i^{C_j} \cdot PN_i + (1 - \alpha) \cdot \sum_{j=n+1}^{n+m} PN_{Oj} \cdot \sum_{i=1}^{k} dt_i^{O_j} \cdot PN_i \tag{2}$$

$$L_p = \alpha \sum_{j=1}^{n} PN_{Cj} \cdot \sum_{i=1}^{k} dp_i^{K_j} \cdot PN_i + (1 - \alpha) \cdot \sum_{j=n+1}^{n+m} PN_{Oj} \cdot \sum_{i=1}^{k} dp_i^{O_j} \cdot PN_i \tag{3}$$

where PN_i – normalized coefficient of the significance of discipline i; PN_{Cj},PN_{Oj}- normalized coefficient of significance competency (discipline group C and discipline group O); α - coefficient of the significance of competency O; n, m – number of competencies C and O accordingly; $dt_i^{C_j}$and $dp_i^{O_j}$ ($dt_i^{C_j}$and $dp_i^{O_j}$) – the total result of competency j cycle of disciplines C and O accordingly; k_1 and k_2 – number of disciplines by realized C and O competencies; k – total number of disciplines.

The type of parameters of the common educational component (readiness indicator) of information security is shown in Table 2.

Different information security initiatives are being carried out to improve the educational component (readiness indicator) of information security specialists. An example of the quest is a game held at Novosibirsk Technical University for students of the direction of information security.

Using role-playing games for information security awareness tasks has many benefits. In addition to the clear task of simulating a real situation, we can also note the removal of psychological barriers in the interaction of players, and gaining access to practical cases that are difficult to integrate into other types of games. In recent years, there are a lot of various types of games based on the use of roles that are widely represented in information security training tasks [2, 4-6, 10]. Tasks used in these types of games must be usually connected in logical chains or performed in quest's form, and also contain keys or a fixed execution scheme. It should be noted that a large number of ethical hacking competitions are organized as Capture The Flag (CTF) in Novosibirsk Technical University. The game takes place in the digital world, while each team must protect and attack vulnerable systems and collect the flags which are alphanumeric strings. Each challenge has a description, related files, or website links, 2 featuring potential hints, and the number of reward points which each participant or team collects after a successful flag submission [2, 4-6,10,13]. Groups or individual participants are trying to collect as many reward points as possible within a certain time. The winner is the individual or the team with the most collected reward points [6].

Table 2
Type of parameters of the educational component (readiness indicator) of information security specialists

Structural units	Indicators	Range
1. Specialty	1.1 Specialty code	'0'-'9'
	1.2 Year of graduation	0000÷9999
2. Theoretical base	2.1 Theoretical level	0÷100
	2.2 Root mean square deviation	0÷100
3. Practical base	3.1 Practical level	0÷100
	3.2 Root mean square deviation	0÷100
4. Adequacy.	4.1 Indicator of adequacy	0÷100
Discipline	4.2 Indicator of discipline level	0÷100
5. Psychological	5.1 Psychological professional suitability indicator 1	'A'-'E'
professional	5.2 Psychological professional suitability indicator 2	'A'-'E'
suitability	5.3 Psychological professional suitability indicator 3	'A'-'E'
	….	'A'-'E'
	5.*n* Psychological professional suitability indicator *n*	'A'-'E'
6. Performance Data	6.1 Record of service	00÷99
	6.2 record of service as a specialist in the field of information security	00÷99
	6.3 Skill level	0÷9
	6.4 Rating in skill level	'A'-'E'
7. Additional education	7.1 Additional educations last year	0000÷9999
	7.2 Number of additional educations	00÷99
	7.3 Additional specialty codes	'0'-'9'
	7.4 Numbers of professional educations	00÷99
	7.5 Scientistic degree	Yes/No/Range
	7.6 Numbers of scientistic degrees	0÷9
	7.7 Academic rank	Yes/No/Range
	7.8 Numbers of academic rank	0÷9

Block 2 is oriented to forming of standardization of every readiness indicator. If the estimation of the quantitative readiness indicators does not cause special problems because of the presence of a large number of mathematical models, then the readiness indicators require special attention, because the object of estimation is characterized by a large degree of uncertainties.

The aim of this block is the formalization and integration of the basic data formed in the process of quality evaluation. The choice of method of construction of member functions depends on the type of the decision task, a complication of receipt of the checked-up information for decision, the authenticity of this information, and also from labor intensiveness of algorithm of treatment of information at the construction of member functions.

Block 3 of the readiness index estimation algorithm assumes a standard procedure for quantitative evaluation of quantitative indicators and a fuzzy evaluation of qualitative indicators.

The resulting evaluation steps are " Generalization and interpretation of the results " (**Block 4**) and " Forming of conclusions and adjustment of model " (**Block 5**).

4. Experimental Part

The technology of formation of qualitative and quantitative indicators in the form of the information security specialist readiness as an element of a trusted environment figure has been tested in Novosibirsk technical university. Students of different specialties (10.03.01 Information security,

10.05.03 Information security of automized systems) took part in this experiment (department information security). Thus, experimental work on the formation of indicators of readiness of specialists in the field of information security was carried out in the period 2020-2021.

The formation of readiness indicators of information security specialists, interaction with employers contributed to increasing the responsibility of all participants in the educational process for the total results. The results of pedagogical monitoring were: a clearer organization of practices, improved educational programs of some disciplines, modified educational and methodological complexes, modernized laboratory installations.

Teachers noted the increased interest of students in the learning process. From these positions, the motivational factor for learning was investigated throughout the training period according to the modified methodology. Table 4.4 presents the structure of educational motivation of students of different groups throughout the entire period of study. In the motivational structure of students, motives related to professional self-realization in the field of information security, as well as educational and cognitive motives, occupied a leading place. These groups of motives for senior students are real and encouraging since they are associated with close professional goals. According to teachers, the awareness of the process of forming an indicator of readiness as a result of the training was an important factor affecting the motivational structure of students in the information security direction

The dynamics of structural elements of the readiness indicator on average (levels of theoretical knowledge, practical skills) are positive. Individual psychological qualities were assessed by specialists of the professional psychological selection group using a set of psychodiagnostic methods and tests taking into account modern requirements for an information protection specialist.

The experts of the commission, when assessing the psychological qualities of specialists in the field of information security, concluded the professional suitability of graduates based on levels of determination, mindfulness, stress resistance, and others.

5. A Conceptual Model with Feedback of E-Employment Operator

To improve the interaction of the modern labor market and the continuous system of employment education, the option of creating federal and regional e-employment operators (FO and RO) was proposed. The conceptual scheme of the electronic employment operator in the modern labor market determines the interaction at two levels: federal and regional. The federal level is implemented by introducing the Federal Economic and Social Fund, the functions of which should include: the creation of single information space for storing and processing personal data, the creation of a state system for ensuring integrated information security, and the organization of bilateral communication with the Federal Economic and Economic Council (processing requests). RO implements the functions of the state computer system with the corresponding services providing it, designed to edit and add indicators of readiness of specialists, and also organizes two-way feedback with the continuous education system and the labor market through the specialist readiness indicator mechanism on request.

Problem stating. Let L be the Federal Electronic Employment Operator (FO); R_j - Regional e-employment operator (RO), where $j = 1..\ n$ (n is the number of regions); S_j^i - graduating educational institutions, where $i = 1..\ m_j$ (m_j is the number of educational institutions); T_j^k - employers' organizations, where $k = 1..\ p_j$ (p_j is the number of employers organizations). It is necessary to build a simplified conceptual model with feedback on the functioning of the e-employment operator in the modern labor market to increase the effectiveness of the interaction between the modern labor market and the continuous education system, the quality and speed of the provision of public employment services (Figure 3).

In the framework of the theoretic-multiple models of the FO and RO, we consider network paradigms (Petri networks and their extensions) of structuring causal connections and modeling systems with parallel processes that serve to stratify and traditive the dynamics and discrete-continuous systems.

The use of Petri networks has proved their validity in various fields: the development of communication protocols, parallel and distributed systems, verification of object-oriented programs, etc. [2]. Modeling in Petri networks is carried out at the event level and is widely used in modeling socially significant areas of human activity.

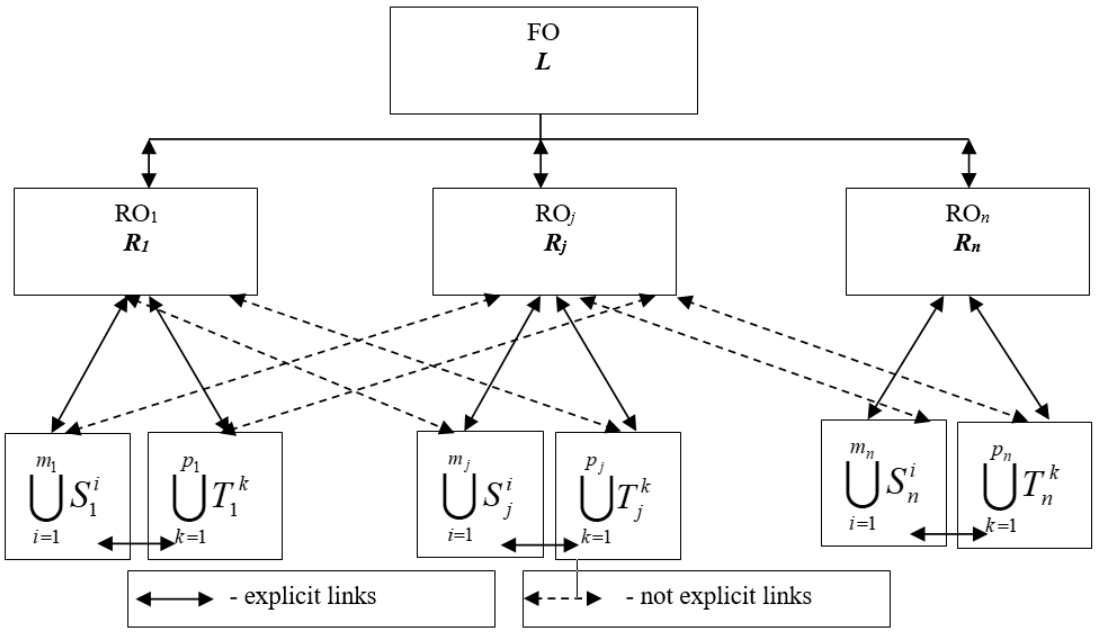


Figure 2: Simplified conceptual model with feedback of e-employment operator functioning in the theoretical-multiple context

The Petri MA network is presented as a tuple of the form (4):

$$< S, TY, IN, OUT >, \quad (4)$$

where S - a non-empty set of educational results, results of competencies formation according to the direction/specialty of training, "Psychophysiological characteristics" (PSFH); $TY=\{t_{ij}, t'_{ij}, y_{ij}, y'_{ij}\}_{2,n1+n2}$ is a finally non-empty set of communications (transitions); IN: $(S\times TY)\rightarrow N$ a set of input one-to-one matching functions of a set of vertices and transitions; OUT: $(S\times TY)\rightarrow N$ a set of output one-to-one matching functions of a set of vertices and transitions in the context of continuous education, namely:

OUT1- The outcome of the general education;

OUT2 - The outcome of the higher education/secondary special education disciplines;

OUT3 - Employment through FO and RO (Figure 3).

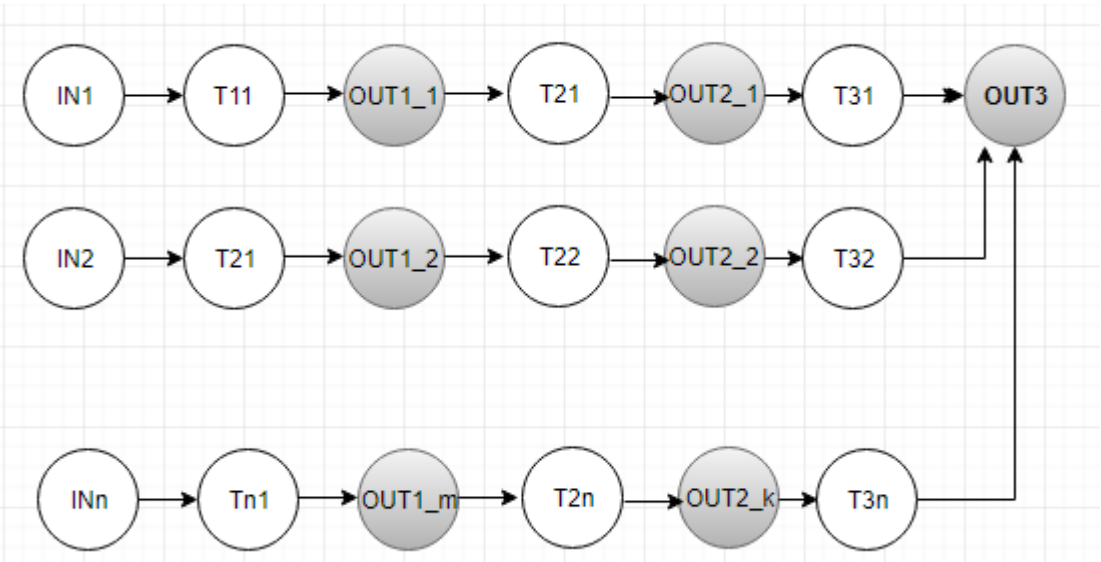


Figure 3: A simulation model of the RO and FO operations in the modern labor market with parameters OUT1-3

A model of the process of forming the threshold level of the applicant of the output function OUT1 is a Petri network with nodes and connections in the form of sets of disciplines, PSFX, and processes of their formation. The initial marking of the network determines the level of the preschool of the educational institution ($IN_1,..IN_n$). Markers of transitions of $TY=\{t_{ij},t'_{ij}, y_{ij}, y'_{ij}\}_{2,n1+n2}$ represent threshold values potentials of studying a complex of disciplines of a set of *TY* according to the list of entrance functions.

6. Conclusions

The article proposes the technology of forming a qualitative and quantitative indicator in the form of an indicator of readiness of an information security specialist as an element of a trusted environment figure. The article proposes also a simulation model of the functioning of the FO and RO in the modern labor market based on the Petri network. The Petri network is a set of functional transitions between node elements, presented in the form of results of specialized educational programs, results of competency formation, psychophysiological characteristics for any training direction/specialty.

The operation of the FO and RO, which are based on the State information system for processing multisociometric components, contributes to the effective and expeditious interactions between the modern labor market and the continuous education system, as well as the timely provision of public employment services.

The proposed algorithm involves Big Data processing. The modern level of informatization allows us to automate the process without any difficulties since the tools of fuzzy mathematics used are easily programmable and do not require specialized hardware. Developed based on fuzzy logic algorithms, the Automated System allows not only to determine the importance of criteria and analyze expert data following them but also to interpret the obtained calculations in the form of recommendations for eliminating identified shortcomings. Also, the proposed information system allows selecting experts to participate in the quality assessment of the assessed system by the expert qualification criteria in the area under consideration, using fuzzy mathematical algorithms [9]. The information system is currently in trial operation. A detailed description of functions and capabilities is not subject to this article and will be submitted upon receipt of the certificate of state registration of software.

Thus, the availability of quality assessments will be useful in the implementation of a coherent, interconnected system of expert actions aimed at achieving the goals and results of evaluation activities at each stage of the generalized algorithm.

When assessing the readiness indicator, the principle of an integrated approach reflects the need to take into account all evaluation criteria, as well as emerging socially significant needs and results of activities in all cycles of individual activity.

7. Acknowledgments

This work was supported by the Vladimir Potanin Foundation for Basic Research project No GK21-001229.

8. References

[1] B. M. Bowen, R. Devarajan, S. Stolfo, Measuring the human factor of cyber security. In: 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 230-235. IEEE, Boston (2011). https://doi.org/10.1109/THS.2011.6107876.

[2] G. Conti, T. Babbitt, J. Nelson, Hacking competitions and their untapped potential for security education. IEEE Security & Privacy, 9(3), 56-59 (2011). https://doi.org/10.1109/MSP.2011.51.

[3] A. Dzhalalov Human factor: philosophy, ideology, politics. Uzbekistan, 1991. 154 pp.

[4] J. Hamari, J. Koivisto, and H. Sarsa, (2014). Does Gamification Work? - A Literature Review of Empirical Studies on Gamification. Proceedings of the Annual Hawaii International Conference on System Sciences. DOI:10.1109/HICSS.2014.377.

[5] M. Hendrix, A. Al-Sherbaz, B. Victoria, Game-based cyber security training: are serious games suitable for cyber security training?. International Journal of Serious Games, 3(1), 53-61 (2016). https://doi.org/10.17083/ijsg.v3i1.107.
[6] S. Karagiannis, E. Maragkos, E. Magkos, An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. IFIP World Conference on Information Security Education, 2020. DOI: 10.1007/978-3-030-59291-2_5.
[7] A. B. Krokhaleva, V. M. Belov, The human factor in the system of socially significant activity (article of the Higher Attestation Commission). Mathematical structures and modeling. 2017. № 4(44). p. 85-99.
[8] Large interpretive dictionary of the Russian language: Ed. Can. philol. sciences S. A. Kuznetsov. St. Petersburg: Norint, 1998. 1534 pp.
[9] Official website of Positive Technologies, 2021. URL: https://www.ptsecurity.com/ru-ru/.
[10] C. Pham, T. Dat Thanh, C. Kenichi, and R. Beuran, CyRIS: a cyber range instantiation system for facilitating security training, Conference: International Symposium on Information and Communication Technology SoICT 2016, December 2016, DOI: 10.1145/3011077.3011087.
[11] G. K. Yuzufovich, S. A. Tsvetkov, Directions, and contradictions of activating the human factor. Human factor and economic progress: Sat. scientific. tr ./Redcol.: G. S. Vechkanov and others; LIEI, 1989. – 160 pp.
[12] V. V. Zolotarev, A. B. Arkhipova, N. Y. Parotkin, A. P. Lvova, Strategies of social engineering attacks on information resources of gamified online education projects. CEUR Workshop Proceedings. 2021. Vol. 2861: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020), Stavropol, 12–13 Nov. 2020. P. 386–391. URL: http://ceur-ws.org/Vol-2861/
[13] S. Kucek, M. Leitner, An Empirical Survey of functions and configurations of open-source capture the Flag (CTF) environments. Journal of Network and Computer Applications, 102470 (2019). https://doi.org/10.1016/j.jnca.2019.102470.
[14] M. R. Martínez-Torres, S. L. Toral Marín, F. B. Garcia, S. G. Vazquez, M. A. Oliva, T. Torres, A technological acceptance of e-learning tools used in practical and laboratory teaching, according to the European higher education area. Behaviour & Information Technology, 27(6), 495-505 (2008). https://doi.org/10.1080/01449290600958965.