Kateryna MOKLIAKOVA[1], Andrii BIGDAN[2], Tetiana BABENKO[3]

MODELE OCENY KOMPETENCJI ZAWODOWYCH AUDYTORÓW BEZPIECZEŃSTWA INFORMACJI

Streszczenie: Metoda oceny kompetencji zawodowych audytorów bezpieczeństwa informacji pracujących z obiektami infrastruktury krytycznej na podstawie certyfikacji zbudowanej z wykorzystaniem modeli Rush oraz doboru binarnego personelu korzystającego z funkcji logistycznej.

Słowa kluczowe: audytor bezpieczeństwa informacji, ocena personelu, obiekty infrastruktury krytycznej, model Rush, selekcja binarna z funkcją logistyczną, sztuczne sieci neuronowe

INFORMATION SECURITY AUDITORS' PROFESSIONAL COMPETENCIES ASSESSMENT MODELS

Summary: A method of assessing the professional competencies of information security auditors that work with critical infrastructure facilities based on certification built using Rush models and Binary selection of personnel using the logistics function**.**

Keywords: information security auditor, personnel evaluation, critical infrastructure facilities, Rush model, Binary selection with logistic function, artificial neural networks

1. Introduction

The profession of information security auditor is design to impartially evaluate the effectiveness of information protection methods usage. The responsibility of knowledge requirements defining, certification (re-certification) of information security auditors is imposed on the public services that deals with information protection and/or special connection regulation. However, the problem of the uncertainty in professional competencies assessment methodology persists in many countries. For example, according to the Regulation [1], the State Service for Special Communications and Information Protection of Ukraine: ensures the implementation

[1]Taras Shevchenko National University of Kyiv, Faculty of Information Technology, Cybersecurity, katerynamok@knu.ua
[2] Assistant, Taras Shevchenko National University of Kyiv, Faculty of Information Technology, abigdan@gmail.com
[3] Doctor of technical sciences, professor, Taras Shevchenko National University of Kyiv, Faculty of Information Technology, babenkot@ua.fm

of the information security audit system at critical infrastructure facilities, sets requirements for information security auditors, their certification (re-certification); coordinates, organizes and conducts audit of security of communication and technological systems of critical infrastructure objects. Nonetheless, there is some uncertainty about the methodology for assessing the professional competencies of information security auditors in Ukraine.
Common competencies assessment methods are described in ISO 19011 [2]. Evaluation criteria includes: specialized educational level, work experience in the information security field, professional qualification (certification), experience in audit conducting, reviews of auditing activities, test results and interviews.

2. Employee hiring process

According to the research [3], each organization during employees hiring process should go through two main stages: selection and election of the candidate. At the selection stage, you need to analyze the needs and scope of the organization, study the market for potential candidates and consider a strategy for finding the right person. In terms of audit of IS of state institutions and critical infrastructure facilities, at the selection stage such criteria should be defined as: the need for the candidate to have access to information with limited access (by law regulation), minimum work experience or educational level, the need for professional certification (e.g. CISA ISACA [4], CIA IIA[5]).

The election stage is divided into stages: analysis of candidates' applications and information provided by them - preliminary selection; conducting interviews and testing. Therefore, when analyzing applications, auditors who do not meet the requirements formed during the selection phase will be eliminated. Interviews and testing focus on assessing the professional competencies of the information security auditor.

3. Certification

Testing is an objective method of an auditor's qualifications determining. For the authority of the test, government agencies should follow one structure. It'll make it easier for either public or private organizations who are looking for the right person to lead an information security audit. Thus, it makes sense to create a general national certification of information security auditors. To do this, it is necessary to develop a database of questions that are created using the approaches of ISACA, ISO 27000 standards family [6], PCI DSS [7], etc., as leading international methods of training and education of auditors and specialists in the field of IS.

To determine the threshold for passing the certification test and the appropriate levels of qualification, a model for assessing the complexity of the questions should be chosen. The item response theory, also known as the latent response theory refers to a family of mathematical models that attempt to explain the relationship between latent traits (unobservable characteristic or attribute) and their manifestations (i.e. observed outcomes, responses, or performance). They establish a link between the properties of items on an instrument, individuals responding to these items, and the

underlying trait being measured. IRT assumes that the latent construct (e.g. stress, knowledge, attitudes) and items of a measure are organized in an unobservable continuum. Therefore, its main purpose focuses on establishing the individual's position on that continuum [8]. Simply saying during the test process it worth considering the surface of other factors than knowledge.

In this case, it is proposed to use the Rasch model [9], which provides valid results by using adequacy statistics, diagnostic information and a correlation map of the level of complexity of tasks with the level of competencies of the certified person.

Requirements for questions, according to the model of Rasch are:

- A measure of the level of preparation of any candidate $t_i \in (0; \infty)$ (regardless of the level of complexity of test tasks);
- The probability of the correct answer P_i- depends on the level of preparedness of the subject and the level of complexity of the test task $b(0; \infty)$ (ie the quantitative characteristics of the test task, which does not depend on the sample and is defined on a scale on a particular section for a particular field of knowledge), or $P = f(t, b)$.

To build a scale of measurements, it is convenient to depict the level of readiness t and the level of complexity b on the logarithmic scale: $\theta = \ln(t)$, $\beta = \ln(b)$, where θ and β are the values of levels of readiness and complexity measured on a logarithmic scale (logits).

Thus, the mathematical function of the probability of "victory" of the subject when answering the questions calculates as (1)

$$P_j(\theta) = \{x_{ij} = 1 \,|\beta_j\} = \exp \frac{\theta - \beta_j}{1 + \exp(\theta - \beta_j)} \quad (1)$$

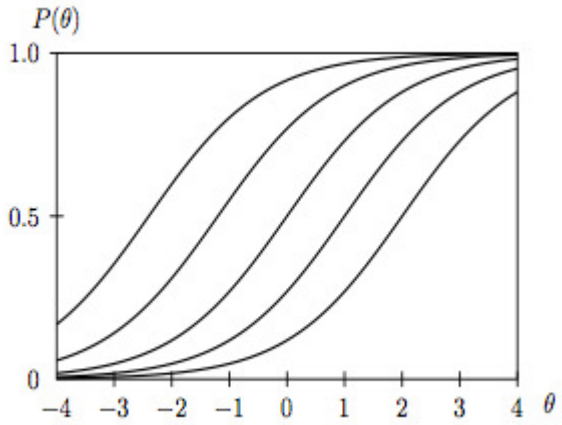

Figure 1. Characteristic curve of the ratio of probability and ability of a person to answer questions.[4]

Therefore, when constructing a test, the distribution of the ratio of preparedness logits and the complexity of one question should increase logarithmically. The adequacy of the questions is determined by the degree of deviation of the empirical points from the characteristic curve (Fig.1). The reason why should we rely on the characteristic curve is because it is used in the method of characteristics for solving partial differential equations.

Based on the participants certification results, it is possible to determine the lower edge of the test score for each proficiency level (low, medium, high), and it is advisable to set a threshold of 60% correct answers as minimum requirement for the test. The division is made to robust categorize process. Therefore, based on certified level organizations can set a minimum degree requirements to gain the best outcome from the desired audit. The quality and level critical infrastructure security depends on the audit results, so the auditor must have a high level of competence. If the applicant has not "passed" the threshold - the test is considered not passed and requires examination retake.

In addition, the education path should be developed for information security auditors with practical and theoretical parts that can prepare young specialists for the entry-level auditor's work. Further implementation of those programs in higher education schools is something to keep in mind as it simplifies the education vector of the need for personnel.

4. Auditors election method

Next to testing, we can identify the following indicators by which the IS auditor is elected: age, higher education, profile (humanitarian/technical), work experience, professional certification, number of organizations and audits, etc. Since the election model must contain a large number of indicators, it is worth using a binary election model with a logistic distribution function, because the value of the parameters is endogenous (takes the value 0 or 1).

Suppose that the variable Y - the possibility or impossibility of taking the position of auditor IB has 2 values of $y = \{0;\ 1\}$. The probability that it will take one of the values is expressed as a function of several factors $x^T = \{x_1, x_2, \dots x_i\}$ (2), (3):

$$P(Y = 1|x) = F(x^T\beta) \tag{2}$$

$$P(Y = 0|x) = 1 - F(x^T\beta) \tag{3}$$

The set of parameters β is the effect of changes in each factor on the final probability. Thus, it is necessary to find an adequate function in the right part of the equation. The logits model of binary search uses the function of the logistic distribution (4):

$$P(Y = y|x) = \exp(x^T\beta)\ /(1 + \exp(x^T\beta)) = \Lambda(x^T\beta) \tag{4}$$

Where $\Lambda(x^T\beta)$ - lambda function of the regression vector (model factors) and function parameters. Estimation of β parameters is carried out by the method of maximum likelihood [10] (5):

$$P(Y_1 = y_1, \dots Y_n = y_n|X) = \prod_{y_i=0}[1 - F(x_i^T\beta)] \prod_{y_i=1} F(x_i^T\beta). \quad (5)$$

The logarithmic likelihood function - L for n observations [11] will have the following form (6):

$$L(\beta|data) = \prod_{i=1}^{n}[F(x_i^T\beta)]^{y_i}[1 - F(x_i^T\beta)]^{1-y_i}. \quad (6)$$

Now the likelihood equation, according to the likelihood function and partial functions - f_i, is (7) :

$$\frac{dLnL}{d\beta} = \sum_{i=1}^{n}[\frac{y_i f_i}{F_i} + (1 - y_i)\frac{-f_i}{(1-F_i)}]x_i = 0. \quad (7)$$

Since these equations are nonlinear, numerous methods are used to solve them, such as a multidimensional interpretation of Newton's method (8):

$$\beta^{j+1} = \beta^j - H^{-1}(\beta^j)gradL(\beta^j) \quad (8)$$

Where L - Lagrangian function (method for finding the conditional extremum of a function), H - Hessian matrix [12] (square matrix of second-order partial derivatives), j –scalar field coordinate.

Features of the binary regression usage to assess the candidate is based on the need for quantitative interpretation of qualitative variables. For example, audit experience may include an assessment of the organizations where it was conducted.

To calculate the result, it is advisable to use artificial neural networks. They can approximate functions, which allows you to build a distribution surface of great complexity, and, consequently, to effectively classify. For instance, it is possible to use the McCulloch-Pitts Neuron model[13] which is the first math model of a biological neuron. Taking several input it provides a single function f result (Fig.2).

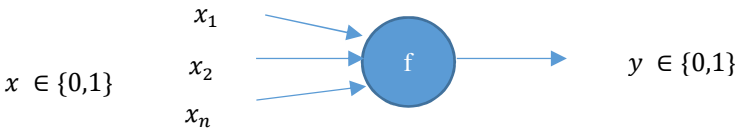

Figure 2. McCulloch Neuron model

One of the disadvantages of intelligent neural networks is that they do not show exactly how individual factors affect the classification. However, studies [3] show that in the artificial neural networks learning process it is the logit models of binary choice that shows the best result. The neural network of this configuration carries out the correct classification for all workers and does not give uncertain estimates.

5. Conclusion

Therefore, to assess the professional competencies of information security auditors and to proceed election of candidates for critical infrastructure and government agencies audits we need to complete next requirements:

- Creation of standardized certification with database of questions built based on international standards and selected according to the Rasch model.

- Usage of a binary selection model to select an IS auditor who will fit the most to conduct a specific audit, including various categories and indicators.
- Automated interpretation of the mathematical model of search using an artificial neural network with previous learning.

As a result, the further researches specified on question database creation and development of neural network with its learning is needed to achieve a comprehensive combined model of information security auditors' professional competencies assessment.

REFERENCE

1. Cabinet of Ministers of Ukraine, "Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine", Normative document
2. ISO/IEC 19011, Normative document, 2018
3. ZINCHENKO A. A.: Modeling of processes of selection and assessment of personnel - Moscow 2015.
4. ISACA: organization *https://www.isaca.org/*
5. The Institute for internal auditors: *https://na.theiia.org/Pages/IIAHome.aspx*
6. ISO 27000 family: *https://www.itgovernance.co.uk/iso27000-family*
7. PCI DSS: https://www.pcisecuritystandards.org/
8. IRT: *https://www.publichealth.columbia.edu/research/population-health-methods/item-response-theory*
9. DEMENCHENKO OG: Mathematical foundations of Rasch Measurement // Pedagogical Measurements, 1(2010).
10. GREENE W. H.: Econometric Analysis / W. H. Greene. – New Jersey : Prentice Hall, 2012.
11. IZENMAN A. J.: Modern Multivariate Statistical Techniques: Regression, Classification, and Manifold Learning Springer / A.J. Izenman. New York: Springer-Verlag, 2008.
12. KAMYNIN L.I. Mathematical analysis. 1,2(2001).
13. CHAKRAVERTY S., SAHOO D.M., MAHATO N.R.: McCulloch–Pitts Neural Network Model. In: Concepts of Soft Computing. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-7430-2_11