Conceptualization of knowledge about information security management system

Mokhor Volodymyr[1]

[1]Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, 15 General Naumov Str., Kyiv UA-03164, Ukraine, v.mokhor@gmail.com

Tsurkan Vasyl[2]

[2]Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, 15 General Naumov Str., Kyiv UA-03164, Ukraine, v.v.tsurkan@gmai.com

Dorohyi Yaroslav[3]

[3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Prosp. Peremohy, Kyiv UA-03056, Ukraine, argusyk@gmail.com

Shtyfurak Yurii[4]

[4]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Prosp. Peremohy, Kyiv UA-03056, Ukraine, yura.shtyfurak@gmail.com

Abstract. *The use of ISO / IEC 27000 and ISO Guide 73 standards as glossaries of terms regarding the information security management system is considered. The establishment of correlation between terms on the ontological approach is shown. Attention is drawn to its applicability to the presentation of organizational guidelines and deadlines for risk. Against this background, conceptualized knowledge about the ontology information security management system, taking into account the systematic approach. This system is presented as a complete entity with stable structural and functional links between its elements.*

Keywords: *information, risk, information security, information security management systems, conceptualization, ontology.*

I. Introduction and Problem statement

Information security management systems are developed using the terms and definitions of ISO / IEC 27000 [1]. At the same time, this glossary is supplemented by terms on risk and risk management in general [2]. Both documents are focused on creating a unified approach to defining and interpreting the concepts of information security management system [1, 2].

The relationships between the terms based on the ISO / IEC 27k series are determined ontologically. Its use makes it possible to establish relationships between security concepts and standards, in particular, ISO / IEC 27001. A characteristic feature of such relationships is the orientation either to the attainment of organizational guidelines or to terms regarding risk (asset, vulnerability, threat, risk). Recommendations for the practical application of such ontologies are given in [3, 4].

II. Problem solution and Results

Knowledge about the information security management system is conceptualized in a systematic approach. It is regarded as a coherent entity consisting of a set of structurally and functionally interrelated elements. The integrity of the object is ensured by a set of strong links between the elements that make up the structure of the information security management system.

The ontology of an information security management system is defined by an interconnected and coherent set of three components [5, 6].

$$O = \langle X, \Re, \Phi \rangle, \quad (1)$$

where O – ontology; X – non-empty finite set of terms regarding the information security management system; $\Re$ – finite set of relations between terms; Φ – finite set of interpreting functions defined in terms and/or relationships of an ontology.

If $\Re = \varnothing$ and $\Phi = \varnothing$, then (1) displays a glossary V of terms according to ISO/IEC 27000, ISO Guide 73 [1, 2, 5, 6]

$$O = \langle X, \{\}, \{\} \rangle,$$

$$O = V.$$

III. Conclusions

Therefore, knowledge about the information security management system is conceptualized using an ontology with a systematic approach. For this purpose, the dictionaries of ISO/IEC 27000, ISO Guide 73 and, secondly, the presentation of the system as a whole entity with a set of structurally and functionally interrelated elements were used.

References

[1] International Organization for Standardization. (2018, Febr. 7). ISO/IEC 27000, Information technology. Security techniques. Information security management systems. Overview and vocabulary. Geneva. [Online]. Available: https://www.iso.org/ru/standard/73906.html.

[2] International Organization for Standardization. (2016, Jan. 21). ISO Guide 73, Risk management, Vocabulary. Geneva. [Online]. Available: https://www.iso.org/standard/44651.html.

[3] I. Meriah, and L. B. Arfa Rabai, "Comparative Study of Ontologies Based ISO 27000 Series Security Standards", Procedia Computer Science, vol. 160, pp. 85–92, 2019, doi: 10.1016/j.procs.2019.09.447.

[4] P. Sirisom, J. Payakpate, and W. Wongthai, "A System Design for the Measurement and Evaluation of the Communications Security Domain in ISO 27001:2013 Using an Ontology", in Information Science and Applications, vol 424, K. Kim, and N. Joukov, Eds. Singapore: Springer, 2017, pp. 257–265, doi: 10.1007/978-981-10-4154-930.

[5] M. Uschold, and M. Gruninger, "Ontologies principles methods and applications", Knowl. Eng. Rev, vol. 11, no. 2, pp. 93–155, 1996.

[6] T. A. Gavrilova, and V. F. Khoroshevskii, Intelligent systems knowledge base, Kharkiv: Piter, 2000.