УДК 004:94

O. Didyk, O. Ohnieva

THE USE OF ONTOLOGIES FOR SOLVING INFORMATION SECURITY TASKS

Annotation. *The basic information security issues and solutions through the use of ontologies and ontology systems are described.*

Keywords*: ontology, ontology systems, informational security, consolidated information.*

Introduction

Today, information regarded as one of the main resources of the social development, and information systems and technologies as a means of increasing productivity and efficiency of people's work. Therefore, information is the most valuable and expensive resource. The problem of information security from the moment of its appearance and to the present state has been a long and largely contradictory path in its development.

Presentation of the main material

Since the process of providing information security is a continuous process, the existing methodology for designing a secure system is an iterative process eliminating the drawbacks found.

In 1996, the classical work of Grusho A.A. and Timonin E.E. "Theoretical fundamentals of information security "expressed and substantiated the thesis that the guaranteed security in the automated system should be understood as a guaranteed performance of a priori specified security policy [1].

Previously, security policy guarantee conditions were formulated in the form of standards. This is the approach used by American computer security experts, having published since 1983 several books of the so-called "rainbow series" standard. In Ukraine, similar documents were adopted by the State Technical Commission [4].

The main problems of information security in computer systems arise because information is not rigidly associated with the carrier. The main factors that make it difficult to solve the problem of information security in PC are as follows:

mass application;

© Didyk O., Ohnieva O., 2017

constantly increasing complexity of functioning;

variety of software for personal computers, architectural solutions and easy adaptation to solve various tasks of users [2].

We can highlight the main types of information security issues:

interception of information (violation of the confidentiality of certain information);

modification of information (editing of the original text of the message and / or its replacement with other information);

substitution of authorship (copyright infringement).

At present, the issue of ensuring the security of consolidated information resources is becoming more and more urgent.

The term "consolidated information" covers various sources of information obtained from several sources and integrated in a consistent manner, that are collectively endowed with signs of completeness, integrity, and consistency, and constitute an adequate information model of the problem area in order to analyze, elaborate and effectively use it in decision making support processes. Therefore, the concept of "competitive intelligence", which is used on parity by some researchers, is still one aspect of holistic processes and information consolidation procedures, namely as a process of formation of an information resource for decision making support [5].

At the same time, consolidated information, with the use of all possibilities, actively operating information resources, is called to develop the technological basis for the creation of an information product, to carry out a qualitative and content-related transformation of information, functionally intersecting in this context with the scientific (production of new knowledge) and management (development of solutions, scenarios) activities.

The protection of consolidated information can be provided in various ways, which include modeling the necessary components of information security, namely:

determining of information resources to be protected;

monitoring of a complete set of potentially possible threats and channels of information leakage;

analysis of vulnerability and risks related to the collection of information and leakage channels;

determining of the requirements for protection system;

selection of means of information security and their implementation;

control of protection system [6].

Thus, consolidated information technologies require information security within a particular institution or organization.

Also, at present, there is a fairly active use of ontological models in various aspects of information security.

Ontology is the presentation in a certain language of knowledge about a certain subject area (environment, world). Ontology is necessarily accompanied by some concept of this area of interest. Often this concept is expressed by identifying the basic objects (individuals, attributes, and processes) and the relationships between them. The determination of these objects and the relationships between them is usually called conceptualization.

The following definition of ontology is generalizing: Ontology is a generally accepted and generally accessible conceptualization of a certain area of knowledge (world, environment) that contains a basis for modeling this area of knowledge and defines protocols for interaction between agents that use knowledge in this area and finally includes agreements on the presentation of the theoretical fundamentals of this area of knowledge [7].

The use of ontological models allows the application of a unified knowledge base that holds the conceptual access control system for information resources, as well as the formal semantics of a modeled system. In this case, due to the combination of such a model with the ontological model of the subject area, it will be possible to determine the rules of access in terms of the domain, taking into account their semantics, and also to make decisions on granting or refusing access on the basis of the results of logical conclusion, which cannot be done using databases.

In general, it is possible to distinguish the following areas of research in this area:

formalization of the subsets of XACML language and use of the logical output to validate the security policies formulated by administrator [8];

use of logical output in existing access control models, such as RBAC (Role Based Access Control) and ABAC (Attributes Based Access Control) [9];

 ISSN 1562-9945

creation of an ontology that defines the conceptual system of the subject area of information security General Privacy Ontology[10], Security Ontology [11], NRL Security Ontology [12].

Conclusion

In the course of the conducted analysis, a generalized description of current problems in the field of information security was made, as well as a classification of types of security threats. It was revealed that one of the most important mechanisms of modern means of providing comprehensive information security is the system of control and differentiation of access to resources, for the implementation of which it is expedient to use ontological models and methods of ontological engineering, which will allow determining access rights based on the logical conclusion.

REFERENCES

1. Grusho A. A. Teoreticheskie osnovy zashchity informatsii. [Theoretical fundamentals of information protection] / A. A. Grusho, E. E. Timonina, 1996. – 106 p. (In Russian)
2. Shangin V. F. Informatsionnaia bezopasnost kompiuternyh system i setei: uchebnoe posobie [Information security of computer systems and networks: manual]/ V.F. Shangin, 2008. – 416 p. (In Russian)
3. Romanets Yu. V. Zashchita informatsii v kompiuternyh setiah i sistemah [Information protection in computer networks and systems] / Yu.V. Romanets, P.A. Timofeev, V.F. Shangin, 2001. – 376 p. – (2). (In Russian)
4. Ab-solut-innovatsii uzhe segodnia. Zashchita informatsii. Problemy zashchity informatsii [Ab-solut-innovations now. Information protection. Information protection problems] Available at: http://ab-solut.net/ru/artickes/probkemi_zashiti.
5. Bondarenko M.F. Informatsionnomu obshchestvu – professionalov v oblasti informatsii (Business Intelligence i Knowledge Management na sluzhbe gosudarstvu) [Professionals in the field of information – for information society (Business Intelligence and Knowledge Management on state service)] / M. F. Bondarenko, S. I. Matorin, E. A. Soloviova Available at: www.it2b.ru/it2b2.view3.page123.html. (In Russian)

6. Kalytych H. I. Konsolodatsia informatsii, znan i mudrosti iak proektuvannia I osnova harmoniinogo postupu Ukrainy [Consolidation of information, knowledge and wisdom as projecting and basis for harmonious progress of Ukraine] [Text] / H. I. Kalytych / Publ., NTI. — 2008. — No. 1. — 51 p. (In Ukrainian)
7. Ontolohiia (informatyka) [Ontology (informatics)] Available at: https:// uk.wikipedia.org/wiki/Онтологія_(інформатика).
8. XACML for authorization// http://xacmlinfo.org/.
9. ROLE BASED ACCESS CONTROL (RBAC) AND ROLE BASED SECURITY Available at: http://csrc.nist.gov/groups/SNS/rbac/index.html.
10. Hecker A. Privacy Ontology Support for E-Commerce / A. Hecker, T. Dillon, C. Elizabeth., 2008.
11. Fenz S., Ekelhart A. Formalizing information security knowledge ASIACCS '09: Proceedings of the 2009 ACM symposium on Information, computer and communications security, ACM, 2009 - 183-194.
12. Kim A, Luo J. Myong K, "Security Ontology for Annotating Resources", Naval Research Lab, NRL Memorandum Report, NRL/MR/5540-05-641: Washington, D.C., 2005 - pp. 51

 ISSN 1562-9945