Procedia Computer Science

Volume 88, 2016, Pages 288–293

7th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2016

Information Security and Expert's Knowledge Autoformalization

Anatoly Malyuk[1,2] and Natalia Miloslavskaya[1]

[1]*National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)*
[2]*Financial University under the Government of the Russian Federation, Moscow, Russia*
{AAMalyuk, NGMiloslavskaya}@mephi.ru

Abstract
To implement the proposed Information Security (IS) Maintenance Concept, the IS experts' knowledge autoformalization algorithm was created as the problems of IS assessment and protection level prediction are based mainly on the experts' informal professional knowledge.

Keywords: information security, unified information security maintenance concept, experts' professional knowledge autoformalization

1 Introduction

Intensive information and communication technologies (ICT) development has led to serious qualitative changes in all spheres of public life. Humankind is actually going through the formation of a new information society characterized by its great reliance on ICT. Information and ICT become the main strategic national resources. The ICT phenomenon sharply increasing the impact of 21st century's society was marked in the Okinawa Charter on Global Information Society adopted by the Group of Eight (G8) on July 22, 2000. At the same time the increasing role of ICT leads to an increase in the information security (IS) threats and brings IS issues to the forefront of the any system security that requires the development of science-based approaches to solving them. These IS threats relate to violation of the established modes of ICT systems usage, infringement of the constitutional rights and freedoms of citizens, malware spread, as well as the usage of modern ICT capabilities for the implementation of hostile, terrorist and other criminal acts. Managing IS correctly requires a comprehensive vision of the issues emerging and informed decision making. Hence, the IS maintenance (ISM) issues and, above all, reliable information protection (preventing its distortion, unauthorized modification, malicious collection, etc.) are now of special urgency.

We refers to *IS of a system (system's IS)* as its quality to be characterized, on the one hand, by its ability to resist the destabilizing effects of external and internal threats, and, on the other hand, by the level of threats posed by its operation to the elements of the system and its external environment. And *ISM* is a complicated process divided into many sub-processes of maintaining the secure (protected)

 Selection and peer-review under responsibility of the Scientific Programme Committee of BICA 2016
© The Authors. Published by Elsevier B.V.

doi:10.1016/j.procs.2016.07.437

state of information, characterized by its confidentiality, integrity, availability, etc. via information protection tools/systems (Malyuk, 2014), (Malyuk, 2015).

Thus the paper is organized as follows. The proposed unified ISM concept is described in section 2. The general ISM processes' model is presented in section 3. IS experts' knowledge autoformalization algorithm is introduced in section 4. The future research area concludes the paper.

2 Unified ISM Concept

The unified ISM concept's structure, worked out by selective integration of the best ISM practices (analyzed in detail in (Malyuk, 2014), (Malyuk, 2015)) and based on the general methodological approaches of the classical systems theory and modelling methods and our extension of these approaches and methods to the specific field of IS, is shown in Fig. 1.

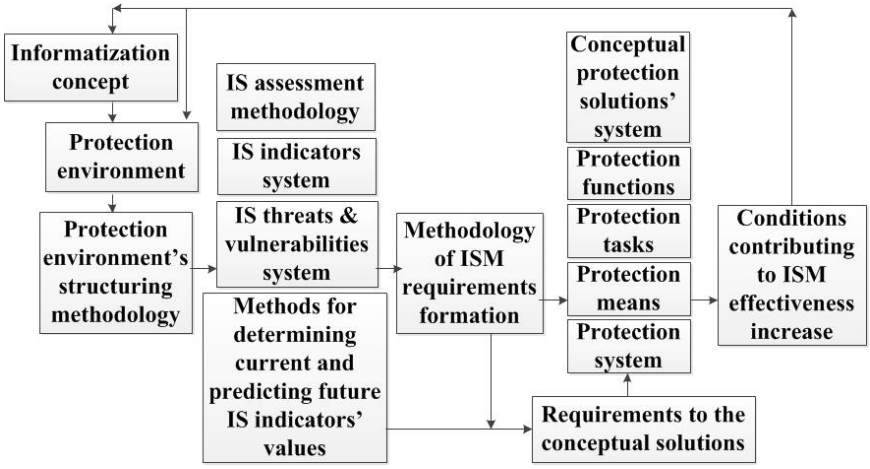

Figure 1: Unified ISM concept's structure

First of all the concepts defining the protection content are developed. They are formed from the concepts of protected automated systems' construction and usage (an informatization concept) and its operation conditions (a protection environment). Further the protection content description is carried out, implying a strictly formal, or, if it is impossible, structured (in the form of a set of interacting elements) representation of the corresponding automated systems' architecture and operation. The IS assessment methodology comprises methods, models and tools to determine the current and predict future values of each of the system's IS indicators under the influence of each of the potential threats and vulnerabilities presence and any their aggregation. The ISM requirements formation methodology determines the approaches, tools and methods of practical organization of information protection. The conceptual protection solutions' system creates objective prerequisites for the formation of various tools and means necessary and sufficient to effectively address the set of the relevant ISM tasks on a regular basis and in accordance with the requirements to their solution which, in turn, are determined by the objectives of the operation of the respective system. The requirements to the conceptual solutions enable to justify such requirements to each of the conceptual solutions that achieve the goals of their adoption in the most rational way. The conditions contributing to ISM effectiveness are required for the formation and study of the list and content of those conditions (including the protection content), compliance with which will significantly increase the protection level in the expenditure allocated for this purpose funds or provide the required protection level while spending the smallest possible amount of funds.

Download English Version:

https://daneshyari.com/en/article/4962276

Download Persian Version:

https://daneshyari.com/article/4962276

Daneshyari.com