Artificial Intelligence in Information Security Systems

V.I. Vasilyev
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vasilyev@vtizi.ugatu.ac.ru

S.S. Valeyev
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vss2000@mail.ru

Abstract[1]

The issues of artificial intelligence application in the tasks of information security are discussed in the paper. A concept of intelligent security system construction on the basis of hierarchical control processes organization is offered. A procedure of complex security system design with use of entropy estimates of risk and information complexity is considered.

1. Introduction

As it is known, an information security is a state of protectivity of the country's national interests (the vital interests of a personality, a society and state) in an information sphere from internal and external threats. Usually a doctrine of homeland security includes three main levels of information security provision [1,2]:

- an information security of the state (protection from cyber-terrorism, critical infrastructure security, security of national information repository etc);
- an information security of society (a city, a firm, an organization);
- an information security of personality (physical protection, security of personal data etc.).

The tasks of first two security levels are characterized by the following features: a high price of decision making; a human factor; a high level of uncertainty; a distributed character of security objects. One of advanced means of security information provision in uncertainty conditions is an application of artificial intelligence methods.

An importance and perspectives of this new direction called as *Intelligence and Security Informatics* (ISI) is mentioned in [3]. Under the leadership of National Scientific Foundation (USA) and IEEE in 2003-2006 in USA there were held several scientific conferences on Intelligence and Security Informatics (ISI'2003-2006) [4]. In 2005 the International Conference on Computational Intelligence and Security (CIS'2005) was held in Hong-Kong (China) [5]. The special issue of IEEE journal "Intelligent Systems" (2005) was devoted to a role and a place of artificial intelligence in solving the homeland security problems including the problem of information security [6].

Main applications in the field of information security being solved with use of artificial intelligence (AI) methods are presented in Table 1.

The analysis of state-of-the art in the field of Artificial Intelligence and Security shows that AI methods today have more and more wide application, e.g.:

- an analysis of virtual enterprises networks (VEN) security [7,8];
- a counteraction to network attacks [9-15];
- a biometric identification [16,17];
- Data Mining in information security systems [18-22];
- a struggle against a spam [23,24];
- Intelligent Building [25] etc.

In all cases mentioned an use of AI methods provides the following advantages:

- an increase of information security tools efficiency in conditions of uncertainty factors (biometric systems, intrusion detection, access control, etc);
- an efficiency increase of information protection tools interaction;
- a maintenance of fault tolerance and survivability of information protection systems ;
- a possibility of prediction of situation change, objectives of information security systems operation, ways of its evolution etc.

Proceedings of the 8th International Workshop on Computer Science and Information Technologies CSIT'2006
Karlsruhe, Germany, 2006

Table 1. Artificial Intelligence Methods and Information Security Applications

Applications	Artificial intelligence methods
- Cryptography and its Applications - Cryptographic Protocols	- Neural networks - Evolutionary Computation - Probabilistic Reasoning - Support Vector Machine - Neural Computing - Molecular Computing
- Detection of Hidden Communication Channels - Detection of Abnormality - Intrusion Detection	- Data Mining - Neural Computing - Fuzzy Systems
- Electronic Commerce Security - Mobile Code & Agent Security	- Machine Learning - Neural Computing - Probabilistic Reasoning - Reinforcement Learning - Swarm Intelligence - Support Vector Machine - Autonomy-Oriented Computing
- Information, Data & System Integrity - Information Hiding - Information Security Management - Information Storage & Retrieval System - Media Data Authentication	- Neural Computing - Unsupervised Learning - Evolutionary Computation - Fuzzy Systems - Intelligent Agents & Systems Data Mining
- Security Models & Architectures - Security Analysis Methodologies - Steganography and Watermarking - Web and Wireless Security	- Intelligent Information Retrieval - Artificial Immune Systems - Biological Computing - Coevolutionary Algorithms

At the same time, as an analysis shows, today practically there are no researches in the field of designing the methodology of intelligent information security systems. This situation does not allow us to use effectively the existing possibilities of AI methods for construction of complex security systems, including information security control systems.

In order to solve this problem, it is necessary to develop a set of models of security objects, threats and vulnerabilities [26,27]. At their construction it is possible to use two different approaches: to build corresponding models on the basis of their description in a form of analytical dependences or on the basis of identification methods. In both cases an essential influence on a model quality is made by factors of uncertainty. The design of information security control system is linked with a number of problems:

- a complexity of analysis and design procedures in a view of a distributed character of security objects;
- a dynamic change of security object structure that demands an analysis and control of information risk in uncertainty conditions.

AI methods are based on applying the knowledge accumulated by experts or extracted from a database that allows using it to solve ill-structured problems of information security.

As basis principles of designing the intelligent systems it is possible to use W.Ashby's principle of a requisite diverse [28] and Saridis's principle of hierarchical organization of a control system ("Intelligent Machine") [29].

With account of said above, we shall consider below a state of a problem of designing the intelligent information security control system for some hypothetic company (firm).

2. Generalized Model of Intelligent Information Security Control System

The generalized structural model of intelligent information security control system is presented in Figure 1 where three levels of control hierarchy are shown: the executive level, the coordination level and the planning level.

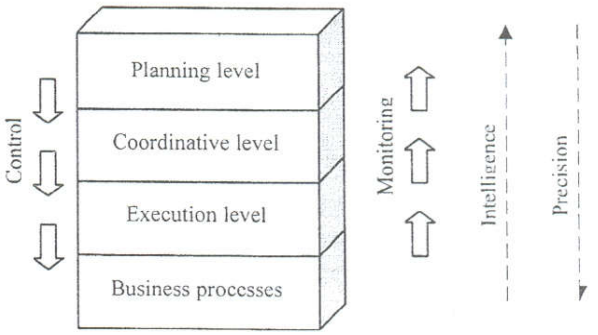

Figure 1. Generalized Model of Intelligent Information Security Control System

The main objective of the executive control level is the maintenance of the required level of information risk at the realization of business processes. The objective of the coordination level is the optimum redistribution of security services among the various subsystems of the executive level and the adaptation of these services properties in case of changing the external or internal conditions (destabilizing factors, threats). The objective of the planning level is decision making for the company mission realization by means of the optimum distribution

of financial and other resources in the framework of the authorized security program. At the development of control decisions, the information on the results of the executive control level, security monitoring at coordination level and objectives of the planning level are used. Thus, the system of information security control can be considered as a hierarchical control system of a distributed dynamic object – business processes of a company.

3. Design of Intelligent Information Security Control System

In order to develop the concept of designing the intelligent information security control system, let's consider a generalized model of such system architecture presented in Figure 2.

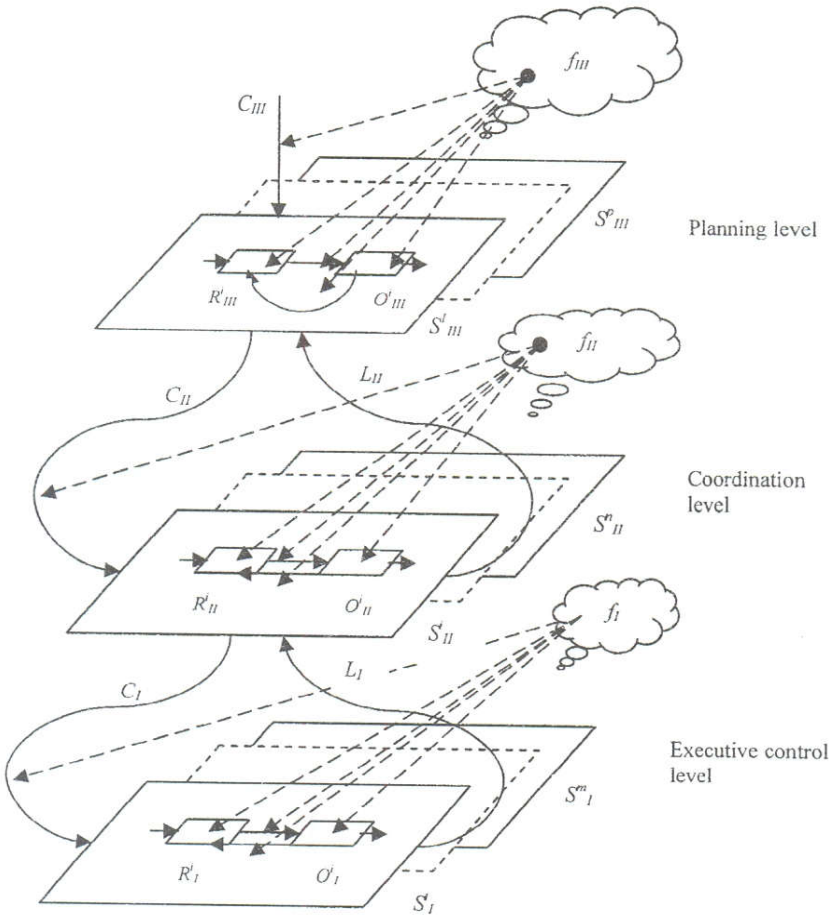

Figure 2. Intelligent Information Security Control System

Here C_j are the objectives of intelligent control system; L_j - the feedback information received on the basis of corresponding information protocols on the results of monitoring of information actives; f_i - the threats of the internal character and from an environment; S^i_j - the *i*-th subsystem of the *j*-th level of intelligent control system; O^i_j - the i-th control object on the j-th level of control; R^i_j - the i-th control system of j-th level of intelligent system (j = I, II, III).

As it is seen, the environment actively influences various levels of this hierarchical system vertical and its horizontal subsystems that in turn through interlevel interaction influences on a security of other hierarchy levels. The processes estimation occurring in the system is necessary for solving the problem of designing the intelligent information security control system at a qualitative level, and estimation of information complexity of the system is necessary for maintenance of economically justified secirity at its various levels.

According to Saridis's principle (*IPDI* principle) [29], the intelligence of the system raises from the bottom to the highest level, and required precision of decision making decreases from the top to the bottom level (see Figure 2). The given principle is one of the basic principles at designing the intelligent information security control system.

The design (algorithmic realization) of the control system on the basis of minimal complexity principle offered by V.Solodovnikov [30] assumes that the choice of control algorithms structure under a change of security object state should be carried out on the basis of optimum using an information and computing resources of the control

system. It in turn can be carried out by means of using an entropy as an universal measure of a system structural complexity [29,31].

4. Procedure of Designing the Intelligent Information Security Control System on the Basis of Information Approach

Let's consider the problem of construction of the mapping $P = (p_1, p_2, p_3)$ from the space of control situations to the space of information security control algorithms. The set of control situations here is defined by the state of information actives (business processes), the state of the threats (environment) and the control objective. The set of control algorithms includes the algorithms used at the listed above three levels of information security: executive, coordination and planning levels. The mapping $P = (p_1, p_2, p_3)$ characterizes the procedure of the choice of security control algorithms on the basis of *IPDI* principle:

$$\text{<Business processes>} \xrightarrow{p_1} \text{<Algorithms of executive level>};$$

$$\text{<Environment>} \xrightarrow{p_2} \text{<Algorithms of coordination level>};$$

$$\text{<Control objective>} \xrightarrow{p_3} \text{<Algorithms of planning level>}.$$

Thus, a complexity of design solutions of intelligent information security control system should correspond to a complexity of considered control situation. As a measure of complexity of control situation in this case it is expedient to use a entropy estimates:

p_1: H (Y/U, F) $\rightarrow C_{exec.}$ \
p_2: H (F) $\rightarrow C_{coord.}$ $\}\Rightarrow$ Entropy as a measure of complexity of design solutions,
p_3: H (G) $\rightarrow C_{plan.}$ /

where Cexec - the complexity of algorithms of the executive level; Ccoord - the complexity of algorithms of the coordination level; Cplan - the complexity of algorithms of the planning level.

Here H (Y/U, F) is the entropy of information security control processes at the executive level; H(F) - the entropy of the threats level changes; H(G) - the entropy of the control objective change; Y,U,F,G - respectivly the vectors of the measured security parameters of business processes, control solutions, external and internal threats, objectives.

The entropy of the vector of business processes parameters in this case is defined as

$$H(Y/U,F) = -\int_{\Gamma_Y} p(Y/U,F)\ln p(Y/U,F)dY,$$

where $p(Y/U,F)$ is the density of probabilities distribution of the vector Y components. The entropy of change of external and internal threats is estimated by the expression

$$H(F) = -\int_{\Gamma_F} p(F)\ln p(F)dF$$

where $p(F)$ is the density of probabilities distribution of the threats vector. The entropy of the control objectives $H(G)$ is estimated similarly.

With account of above stated, the problem of optimum design of three-level intelligent information security control system on the basis of the entropy approach is formulated as follows.

The problem statement. It is required to find such way of design of intelligent information security control system: $U_{opt} = f(Y, F, G)$, i.e. to define the structure of countermeasures, the structure of the database and knowledge base at various levels of the control system providing the requirement $\|Y - G\| \le \varepsilon$ where G is the vector of control objectives to be carried out; ε - the given level of business processes risk in accordance with the given components of the objectives vector G, under the condition of the following restriction

$$H_\Sigma(A) \rightarrow \min.$$

Here $H_\Sigma(A)$ is the total entropy of control algorithms (A) for all control levels of intelligent system which by virtue of relative independence of these levels can be counted up as

$$H_\Sigma(A) = H(A)_{exec.} + H(A)_{coord.} + H(A)_{plan.}$$

where $H(A)_{exec.}$, $H(A)_{coord.}$, $H(A)_{plan}$ are respectively the values of the entropy for algorithms of the executive, coordination and planning levels of intelligent information security control system.

5. Conclusions

The analysis of state-of-the art of research in the area of *Intelligence and Security Informatics* is performed. The concept of designing the intelligent information security control system on the basis of IPDI principle and minimal complexity principle is offered. The procedure of designing the intelligent information security control system with use of entropy complexity estimates for all levels of control system is considered.

References

1. Information Security Doctrine of the Russian Federation. Moscow, Russia, 2000.
2. "Defending America's Cyberspace". National Plan for Information Systems Protection, Version 1.0. The White House, USA, 2000.
3. Lin L., Geng X., Whinston A.B. "Intelligence and Security Informatics: An Information Economics Perspective". In: *Proc. of the 1st NSF/NIJ Symp. "Intelligence and Security Informatics"*. Springer Verlag, 2003, pp. 375-378.
4. http://www.isiconference.org

5. http: // www.comp.hkbu.eduhk / ~ cis05/home

6. "Artificial Intelligence in Homeland Security". *IEEE Intelligent Systems*, 2005; 5.

7. Valeyev S.S., Bakirov T.K., Pogorelov D.N., Starodumov I.V. "Multi-agent Technology and Information Security Systems". In: *Proc. of the 7th International Workshop on Computer Science and Information Technologies (CSIT'2005)*. USATU, Ufa, Russia, 2005, pp. 195-199.

8. Valeyev S.S., Pogorelov D.N. "Information Security in CALS-Technologies". In: *Proc. of the 7th International Workshop on Computer Science and Information Technologies (CSIT'2005)*. USATU, Ufa, Russia, 2005, pp. 207-209.

9. Vasilyev V.I., Khafizov A.F. "Application of Neural Networks to Detection of Attacks on Computers in Internet (on Example of Attack SYNFLOOD)". *Neurocomputers: development, application.* Radiotechnika Pub., 2001; 4-5: 108-114.

10. Vasilyev V.I., Khafizov A.F. "Neural Network Systems of Intrusion Detection for WWW-server". *USATU Transactions*, Vol. 6, 2005; 1(12): 116-120.

11. Mu C., Huang H., Tian S. "Intrusion Detection Alert Verification Based on Multi-level Fuzzy Comprehensive Evaluation". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 9-16.

12. Karim A. "Computational Intelligence for Network Intrusion Detection: Recent Contributions". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 170-175.

13. Yeom K., Park J. "An Immune System Inspired Approach of Collaborative Intrusion Detection System Using Mobile Agents in Wireless Ad Hoc Networks". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 204-211.

14. Ma L., Yang L., Wang J. "Attack Scenario Construction Based on Rule and Fuzzy Clustering". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 328-333.

15. Seo H., Cho T. "Application of Fuzzy Logic for Distributed Intrusion Detection". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 340-347.

16. Li B., Yin H. "Face Recognition Based on Support Vector Machine Fusion and Wavelet Transform". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 764-770.

17. Ivanov A.I. "Neural Network Algorithms of Biometric Identification of Person". Radiotechnika Pub., Moscow, Russia, 2004.

18. Wu L., Su K., Chen Q. "Model Checking Temporal Logics of Knowledge and Its Application in Security Verification". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 349-355.

19. Yeom K., Park J. "An Approach of Information Extraction from Web Documents for Automatic Ontology Generation". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 450-457.

20. Lin L., Liotta A., Hippisley A. "A Method for Automating the Extraction of Specialized Information from the Web". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 489-494.

21. Zeng Y., Ma J. "Sampling Distance Analysis of Gigantic Data Mining for Intrusion Detection Systems". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 228-235.

22. Cui S., Feng B.A. "Fuzzy Integral Method to Merge Search Engine Results on Web". *Lecture Notes in Artificial Intelligence (LNAI)*, 3802, pp. 731-736.

23. Kim J., Kang S. "Feature Selection by Fuzzy Inference and Its Application to Spam-Mail Filtering". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 361-366.

24. Cheng X., Ma X., Wang L., Zhong S. "A Mobile Agent Based Spam Filter System". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 422-427.

25. Park J., Choi J., Lee S., Park H., Lee D. "User-Oriented Multimedia Service Using Smart Sensor Agent Module in the Intelligent Home". *Lecture Notes in Artificial Intelligence (LNAI)*, 3801, pp. 313-320.

26. Gerasimenko V.A. "Information Protection in Automated Systems of Data Processing", Vol. 1-2. Energoatomizdat Pub., Moscow, Russia, 1994.

27. Zegjda D., Ivashko A. "Fundamentals of Information Systems security". Hot Line - Telecom Pub., 2000.

28. Ashby W.R. "An Introduction to Cybernetics". Chapman Hall LTD, London, UK, 1957.

29. Saridis G.N. "Hierarchically Intelligent Machines". World Scientific Pub., Singapore, 2001.

30. Solodovnikov V., Tumarkin V. "Complexity Theory and Design of Control Systems". Nauka Pub., Moscow, Russia, 1990.

31. Vasilyev V.I., Valeyev S.S. "Estimation of Neural Network Models Complexity on the Basis of Entropy Approach". In: Proc. of the 6th Workshop on Computer Science and Information Technologies (CSIT'2004), Vol. 1. Budapest, Hungary, 2004, pp. 38-42.