UDC 004.45: 004.89: 681.3

S.V. GLADYSH

Odessa National Academy of Telecommunications, Ukraine

INFORMATION SECURITY INCIDENT-TOLERANT IMMUNE-INSPIRED MULTI-AGENT SYSTEM

Information Systems and Infocommunication Networks are considered as “organisms” according to the point of view of “Organismic Approach”, Bionics, Bioinformatics, and Evolution Theory. Principles of information security incidents management are defined and inspired by Immunology and Immunocomputing. A concept of an Immune Multi-Agent System for information security incidents management is proposed. The schemes of structure and functions of such a system are developed.

Agent, Artificial Immune System, Incident, Information Security, Infocommunication Network, Management

Introduction

The problem of information security (ISec) incidents management in information and telecommunication systems is similar to the problem of living organism defense from external and internal pathogens.

In general, the principle of bio analogy, as it applies to the tasks of telecommunication networks security, was formulated in the article [1]. Possibilities of its practical use were analyzed in [2, 3].

With respect to the immune system as a source of ideas and methods for ISec tasks - there are two common research directions: 1) artificial immune systems for anomaly detection in software behavior [4, 5] and artificial immune systems for new computer viruses recognition [6].

However, implementation of the immune-inspired approach to the automation and intelligence of ISec incidents management remains an actual task.

Development of structure and functions of the immune multi-agent system for ISec incidents management is the purpose of the given research.

1. Biologically inspired incident-tolerance principles

Actuality of ISec incidents problem and ineffectiveness of its solving by use of the modern methods cause the necessity of new approaches searching and implementation.

“Organismic approach” was initially proposed by academic N. N. Moiseev within the framework of his interdisciplinary research in early 1980th [7].

Applying to ISec incidents management in infocommunication networks (ICN) this approach should mean going out from “technological mechanicism” to a new synergetic understanding, when an ICN is considered as a self-developing system examined through the prism of the evolution theory.

Natural immune systems of living organisms are the structurally-complex adaptive decentralized and distributed systems for information processing and analysis [4, 5]. In this research their basic ability will be considered as: cells and molecules recognition as “self” or “non-self” with further classification and stimulation of the corresponding protection mechanisms.

Growing increase of registered ISec incidents number and their seriousness makes designing and modeling of survival, evolution and adaptation of ICN an actual scientific task. According to such a metaphor an ICN is likened to a biological organism aspiring to survive in a certain natural environment (biocenoze) (fig. 1). Thus the role of an ISec incidents management system could be given to an artificial immune system.

2. Concept of immune multi-agent system

Within the network-organizational architecture of an ICN we will separate and emphasis an automated subsystem for ISec incidents management. Let's design this subsystem by use of multi-agent technology [8].

Consider 4 classes of agents (fig. 1): agents-detectors; agents-identifiers; agents-coordinators; agents-reactors.

1.) Agents-detectors correspond to macrophages and others antigen-presenting cells which allocate the particles of antigen on their surface, attracting B- and T-lymphocytes for recognition. 2.) Agents-identifiers correspond to B-lymphocytes which recognize an antigen. 3.) Agents-coordinators correspond to T-lymphocytes, which could catalyze or inhibit the activating of B-lymphocytes with antibodies and phagocytes. 4.) Agents-reactors correspond to antibodies and phagocytes which eliminate an antigen.

Agents-lymphocytes in order to produce an integral "organism" should provide the homeostasis adjusting control of an ICN as a whole. In the considered context the term "homeostasis control" includes ISec incidents management and ICN maintenance characteristics adjusting in the limits, providing ICN security, quality, reliability and survivability.

Applying of evolutional theory must be realized considering its basic postulates, which could be formulated in this article as follows: a) **expedience**: survive only those ICN, which are the most meet to the environment conditions (incidents); b) **adaptation**: changes in an ISec architecture should be intended for adaptation to the dynamically changing conditions (incidents); c) **self-organization**: processes of ICN evolution result in continuous complicating of its structure and dynamic reallocation of ISec resources and functions, including incidents management.

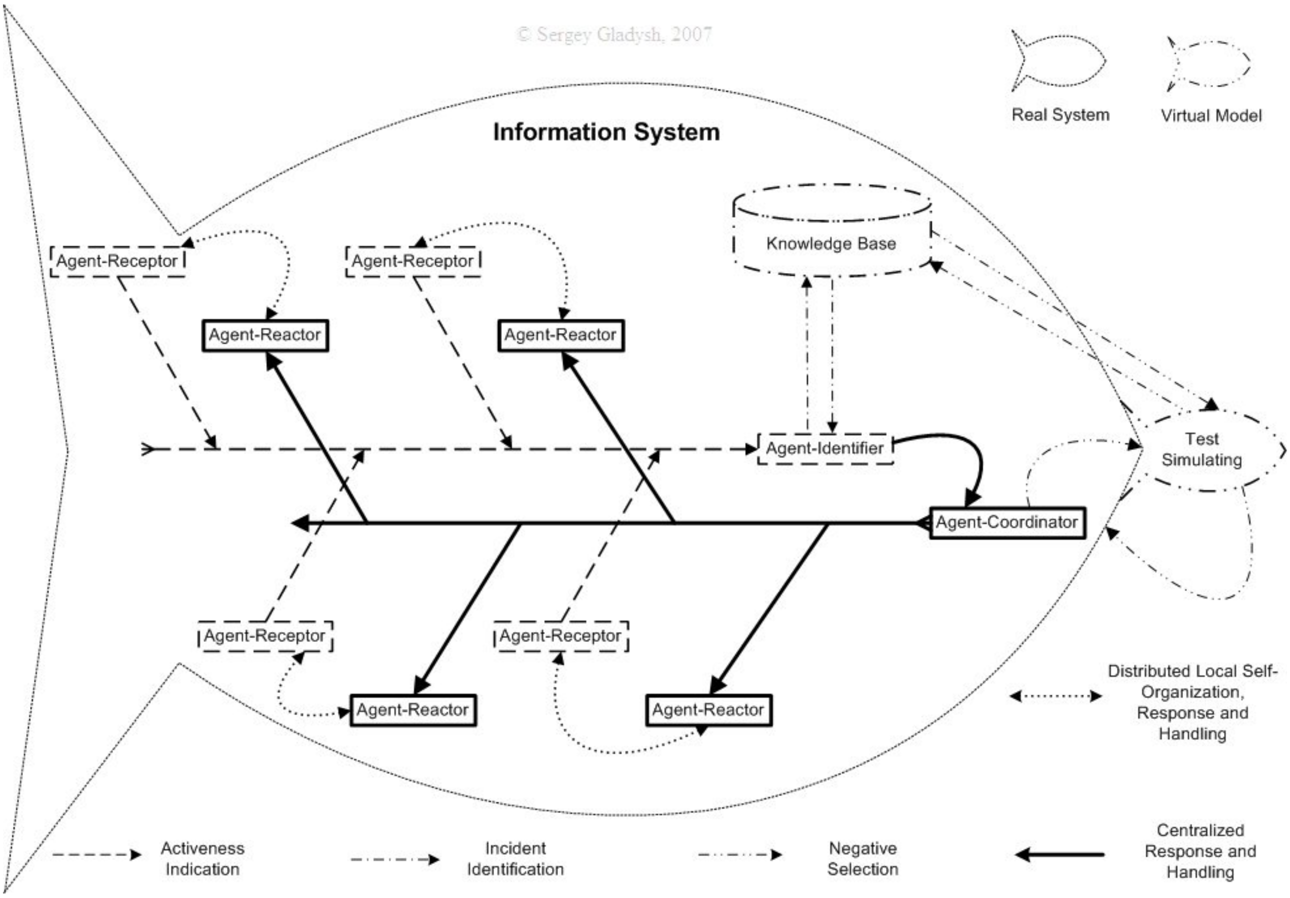

Fig. 1. The Structure of Immune Multi-Agent Information Security Incident Management System

3. Structure and functions of immune multi-agent ISec incidents management system

Let’s define some new concepts which will occur in use further during the present research:

Full Security Mechanisms Set (FSMS) - is a full set of all existent ISec mechanisms.

Agent-Oriented Security Mechanisms Subset (AOSMS) - is a subset of ISec mechanisms from FSMS, which a concrete multi-agent system has under control.

Incident-Oriented Security Mechanisms Subset (IOSMS) - is a subset of ISec mechanisms from AOSMS, which a concrete multi-agent system has under control, and which all together aggregated are sufficient for effective handling of the concrete ISec incident type.

Test Security Mechanisms Subset (TSMS) - is a subset of ISec mechanisms, which are being chosen among AOSMS for simulating, prognosis and adaptation to a known / unknown incident type to produce IOSMS.

Full Threats Set (FTS) - is a full set of all existent ISec threats, which if realized could result in an incident.

Incident’s Attacking Threats Subset (IATS) - is a subset of ISec threats from FTS, which are actual in a concrete ISec incident type.

Processes of ISec incidents management are strongly interconnected with intrusion detection processes. Therefore we will consider the immune multi-agent system for ISec incidents management in tightly cooperation with the Intrusion Detection Subsystem (IDS), because IDS gives out an initial signal about an incident, and from this IDS signal further response and handling of ISec incident begins.

On this basis, we could represent the functional structure of the immune multi-agent system for ISec incidents management (fig. 2).

Agents will interact within the framework of 6 hierarchical subsystems: IDS; incidents identification knowledge base; incidents response subsystem; incidents handling knowledge base; incidents handling subsystem; forensics and feed-back subsystem.

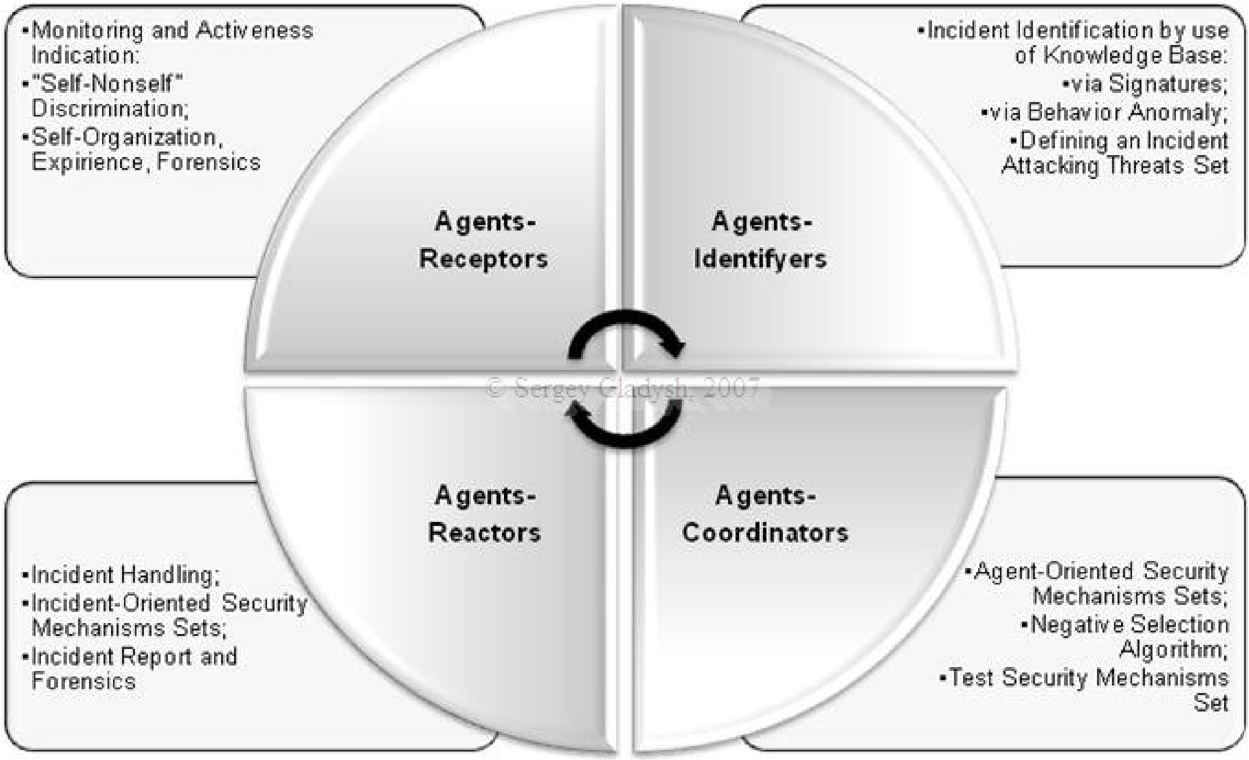
•Monitoring and Activeness Indication:
•"Self-Nonself" Discrimination;
•Self-Organization, Expirience, Forensics
•Incident Identification by use of Knowledge Base:
•via Signatures;
•via Behavior Anomaly;
•Defining an Incident Attacking Threats Set
Agents-Receptors
Agents-Identifyers
© Sergey Gladysh, 2007
Agents-Reactors
Agents-Coordinators
•Incident Handling;
•Incident-Oriented Security Mechanisms Sets;
•Incident Report and Forensics
•Agent-Oriented Security Mechanisms Sets;
•Negative Selection Algorithm;
•Test Security Mechanisms Set

Fig. 2. Functions of Immune Multi-Agent Information Security Incident Management System

Let's define the following stages of ISec incidents management:

1) any suspicious (strange) activity indication by agents-detectors;

2) abnormal activity recognition by agents-identifiers as a certain incident type in case of corresponding signature found in the knowledge base or anomaly detection in comparison with a normal behavior etalon;

3) Response Subsystem receiving an emergency signal from IDS about an identified known or unknown incident;

4) IATS identification in case of correlation between the emergency signal about an incident and IATS records in the knowledge base;

5) TSMS forming according to an algorithm which is stored in or generated by a knowledge base;

6) simulation of eliminating IATS by use of TSMS;

7) decision-making on IOSMS choosing;

8) Handling Subsystem generate the managing signal on ISec incident handling by use of IOSMS;

9) incident forensics, self-organization and IOSMS efficiency evaluation by the feed-back subsystem and agents-detectors, knowledge base extending by adding new experience, decision-making on preventive actions.

Conclusions

In the given article it has been described, how the immune-inspired principles could be used applying to ISec incidents tolerance. Concept, structure and functions of ISec incidents management system have been developed by use of agent-oriented approach. And it has been illustrated, how this could help to achieve a new level of real-time dynamical adaptation and self-organization in ISec incidents management. In order to formalize the task the new concepts and terms have been defined. By using this concepts, structure and functions it has been considered the stages of ISec incidents management.

References

1. Gladysh S. V. Bio-analogy principle use for synthesis of telecommunications security intelligence control systems // Legal, Normative and Metrological Maintenance of Information Security Systems in Ukraine. – 2006. – No. 13. – P. 57 - 63.

2.Gladysh S. V. Biological and medicine analogy principle in knowledge representation models of telecommunications security intelligence control systems // Proceedings of IV International scientific conference «Information Technology and Cybernetics Serving Health Care». – Dnepropetrovsk, Ukraine, 2006. – P. 21 - 24.

3. Gladysh S. V. A multi-agent immune approach to information security assurance in telecommunications // Proceedings of IV International scientific conference «World of Information and Telecommunications - 2007». – Kiev, Ukraine, 2007. – P. 113.

4. Forrest S., Dasgupta D. Novelty Detection in Time Series Data using Ideas from Immunology // Proc. of the 5th Int. Conference on Intelligent Systems. – Reno, June 1996.

5. Dasgupta D. Using Immunological Principles in Anomaly Detection // Proc. of ANNIE'96. - St. Louis, Nov.1996.

6. Kephart J. Biologically inspired defenses against computer viruses // Proc. of IJCAI'95. - Montreal, Aug. 1995. – P. 985 - 996.

7. Moiseev N. N. Universal Evolutionism and Co-Evlution // Nature. – 1989. – No.4. – P. 3 - 8.

8. Gladysh S. V., Kononovich V. G. Response and handling of information security incidents by a multi-agent system // Scientific works of Odessa National Academy of Telecommunications. – 2007. – № 2. – P. 48 - 53

Поступила в редакцию 03.01.2008

Рецензент: канд. техн. наук, доцент, В.Г. Кононович, Одесская национальная академия телекоммуникации, Одесса.