ANALYSIS OF INFORMATION SECURITY METHODS IN BIOSYSTEMS AND APPLICATION OF INTELLIGENT TOOLS IN INFORMATION SECURITY SYSTEMS

Sherzod Sayfullaev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Address: 108, Amir Temur st., 100200, Tashkent city, Republic of Uzbekistan E-mail: sherzodsay@gmail.com, Phone:+998-91-162-42-70., sherzodsay@gmail.com

Follow this and additional works at: https://uzjournals.edu.uz/ijctcm

Part of the Complex Fluids Commons, Controls and Control Theory Commons, Industrial Technology Commons, Other Computer Engineering Commons, Process Control and Systems Commons, and the Systems and Integrative Engineering Commons

Recommended Citation
Sayfullaev, Sherzod (2020) "ANALYSIS OF INFORMATION SECURITY METHODS IN BIOSYSTEMS AND APPLICATION OF INTELLIGENT TOOLS IN INFORMATION SECURITY SYSTEMS," Chemical Technology, Control and Management: Vol. 2020 : Iss. 3 , Article 12.
DOI: https://doi.org/10.34920/2020.3.72-77
Available at: https://uzjournals.edu.uz/ijctcm/vol2020/iss3/12

This Article is brought to you for free and open access by 2030 Uzbekistan Research Online. It has been accepted for inclusion in Chemical Technology, Control and Management by an authorized editor of 2030 Uzbekistan Research Online. For more information, please contact sh.erkinov@edu.uz.
ANALYSIS OF INFORMATION SECURITY METHODS IN BIOSYSTEMS AND APPLICATION OF INTELLIGENT TOOLS IN INFORMATION SECURITY SYSTEMS

Sayfullaev Sherzod
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Address: 108, Amir Temur st., 100200, Tashkent city, Republic of Uzbekistan
E-mail: sherzodsay@gmail.com, Phone:+998-91-162-42-70.

Abstract: In this paper, the methods of information protection in bio systems are studied. The paper considers the use of intelligent tools in information security systems and the use of adaptive information security systems. Several articles on the field of information protection in bio systems are analyzed. Disadvantages and advantages of neural network technologies in modern information security systems are described. The characteristics of bio systems and the specificity of DNA, the main features of the DNA code that provide information security and functional stability of bio systems data protection structure. Application of intelligent tools to create a comprehensive adaptive protection of IT systems based on biosimilar.

Keywords: information technology, neural networks, information protection systems, biological systems, fuzzy systems, DNA, adaptive systems.

Introduction
The evolution of information processing media is carried out in the direction of creating information technology (IT) systems with elements of self-organization, in which there are processes of origin, adaptation and development [1]. On these processes are based biological systems, which are characterized by the experience of evolution, selective selection. Borrowing the architectural principles of bio systems has led to the development of theories of neural networks (NN), fuzzy sets, and...
evolutionary methods underlying artificial intelligent systems.

For the implementation of these processes in technical systems, fuzzy computing methods are being improved which are based on the knowledge of experts and have proven themselves well in conditions of incomplete reliability and uncertainty of information. Optimization problems are solved using evolutionary methods, including genetic algorithms. Neural network technologies provide adaptive tools for implementing IT systems.

The main direction of development of information secure IT systems can be considered the creation of adaptive information protection systems (IPS), convenient for technical implementation with the use of modern Nano electronic technologies [2] in the form of ultra-large integrated circuits (VLSI), silicon wafers focused on highly reliable mechanisms of life support and information protection of biological systems.

High performance of IT systems when solving tasks characterized by fuzzy, unreliable information, irregular processing processes with components that change in composition and interconnections during system operation, can be provided by parallelism of neural network computing and data flow control (DFT). Such calculations are necessary for managing and ensuring information security of complex complexes based on adaptive IT systems with secure processes for processing and storing large amounts of confidential information.

**Research Methods and the Received Results**

Scientific and technical publications [3] actively discuss the need to give information security systems in it the evolutionary qualities inherent in bio systems, such as the possibility of development and adaptability. Well-known companies, such as Microsoft, claim to use "active protection technology" [4], based on evaluating the behavior of programs in terms of their potential danger. In particular, IPS adjust the computer's security корректируют tools when its status changes, or block it if it is suspected of being infected by a virus or an intruder [5].

Most publications on the application of intelligent information security systems are devoted to attack detection systems [6], which typically use neural networks (NN), fuzzy logic systems, and rule-based expert systems as intelligent tools [7, 8].

Attack detection schemes are divided into two categories: 1) abuse detection and 2) anomaly detection. The former include attacks that exploit known vulnerabilities in the IT system, and the latter include activities that are unusual for users of the IT system. To detect anomalies, an activity is detected that differs from the templates set for users or groups of users. Anomaly detection is usually associated with creating a database that contains profiles of controlled activity [9], and abuse detection is associated - with comparing user activity with known hacker behavior patterns [10, 11] and using rule-based methods that describe attack scenarios. The detection mechanism identifies potential attacks if the user's actions do not match the established rules.

You can distinguish the following possible applications of NN in attack detection systems. Adding a neural network to existing expert systems to filter incoming messages in order to reduce the number of false positives inherent in the expert system. Since the expert system only receives data about events that are considered suspicious, the system's sensitivity increases. If the NN identifies new attacks through training, then the expert system should also be updated. Otherwise, new attacks will be ignored by the expert system, whose previous rules are not able to recognize this threat.

If the NN is a separate attack detection system, it processes traffic and analyzes information for abuse. Any cases that are identified with an indication of an attack are forwarded to the security administrator or used by the automatic attack response system. This approach has an advantage in speed over the previous approach, because there is only one level of analysis, and the system itself has the property of adaptability. NN is also used in cryptographic data protection systems to store cryptographic keys in distributed networks [12].

The main disadvantage of the NN is considered the “opacity” of forming the analysis results [13]. However, the use of hybrid neuro-expert or neuro-fuzzy systems makes it possible to explicitly
reflect in the structure of NN a system of fuzzy predicate rules, which are automatically corrected in the process of NN training [14]. The adaptability property of fuzzy NN allows you to solve not only individual tasks of identifying threats, comparing user behavior with existing templates in the system, but also automatically generate new rules when changing the threat field, as well as implement a system for protecting information in the technical system as a whole.

The best combination of properties to achieve this goal is fuzzy NN, which combines the advantages of NN and fuzzy logic, based on the experience of information security experts. The mechanism of fuzzy logical inference allows using the experience of experts, embodied in the form of a system of fuzzy predicate rules, for preliminary training of fuzzy NN [15]. Follow-up training NN in the field of known threats provides an opportunity to analyze the logical inference process for correcting, existing, or synthesizing a new system of fuzzy predicate rules of IPS [16, 17].

Let's list the properties of fuzzy NN that are necessary for adaptive IPS (Fig. 1):

1) functional stability and security of the element base;
2) ability to classify threats;
3) description of the "threats — protection mechanisms" correspondence in the form of a system of fuzzy predicate rules;
4) adaptability of the neuro-fuzzy IPS (fuzzy rules system);
5) "transparency" for analyzing the structure of connections between neuro-fuzzy IPS and a system of fuzzy rules;
6) distributed computing parallelism.

The biosphere — is a hierarchical information system with a unified approach to methods and methods of information transformation, storage and transfer, which have high security. A variety of specialized subsystems of the information technology system, which differ in the complexity of the structural organization and properties, can be brought into line with the diversity of life forms and forms of existence.

In other words, the biosphere is a complex information system, whose subsystems have a set of mechanisms and properties that give them high information security. Ensuring a high level of protection and viability of species is due to the reliability of the method of encoding, storing and transmitting information (in the process of reproduction) - the genetic code of the species.

<table>
<thead>
<tr>
<th>Properties of fuzzy NN that are necessary for adaptive IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>functional stability and security of the element base</td>
</tr>
<tr>
<td>ability to classify threats</td>
</tr>
<tr>
<td>description of the &quot;threats — protection mechanisms&quot; correspondence in the form of a system of fuzzy predicate rules</td>
</tr>
<tr>
<td>adaptability of the neuro-fuzzy IPS (fuzzy rules system)</td>
</tr>
<tr>
<td>&quot;transparency&quot; for analyzing the structure of connections between neuro-fuzzy IPS and a system of fuzzy rules</td>
</tr>
<tr>
<td>distributed computing parallelism</td>
</tr>
</tbody>
</table>

Figure 1. Properties of fuzzy NN.

Giving IT systems the positive qualities of bio systems and, above all, those responsible for the security of information processes, is associated with the presence of:

- hierarchies of functionally heterogeneous subsystems with advanced protection functions,
- information-secure mechanisms for storing and transmitting information,
- properties of a complex cybernetic system,
- evolutionary qualities, namely: the ability to originate, grow and develop, learn and adapt in
a dynamic external environment.

The security of the bio system is provided by mechanisms of heredity and variability, which are informational in nature. The genetic material of bio objects is DNA-deoxyribonucleic acid [2] (Fig. 2).

*Figure 2. Structure of DNA.*

Populations exist through reproduction, which is reduced to the transmission of genetic information within the species through DNA. DNA plays the role of a universal and secure information carrier. The specificity of DNA lies in its dual nature: on the one hand, as a protected information carrier, and on the other - the information itself in the form of a genetic code.

DNA molecules (Fig. 3) are linear macromolecules in the form of double chains of polymers made up of nucleotides, each of which contains one molecule of phosphoric acid (f) and sugar, and it is also one of the four nitrogenous bases: adenine-A, guanine-G, cytosine-C and thymine-T. Adenine and guanine are purine bases, and cytosine and thymine are pyrimidine bases. Combinations of three adjacent nucleotides in the DNA chain (triplets, or codons) make up the genetic code. Violations of the sequence of nucleotides in the DNA chain lead to hereditary changes in the body - mutations. DNA is accurately reproduced during cell division, which ensures the transmission of inherited traits and specific forms of metabolism in generations [2].

The reliability of the structure of DNA is due to the reliability and strength of hydrogen bonds between the chains, and the uniqueness - the fact that species diversity in nature is based on 20 amino acids the genetic code.

DNA studies have revealed a number of patterns (Chargaff's rules):

- The number of nucleotides containing purine bases is equal to the number of nucleotides containing pyrimidine bases \( A + C = T + G \);
- In DNA, the content of adenine is equal to the content of thymine, and the content of guanine
is equal to the content of cytosine \( A = T, G = C, G + T = A + C \);

- The DNA of different species may differ due to the predominance of adenine over guanine and thymine over cytosine \( A + T > C + G \), and vice versa \( C + G > A + T \).
- The ratio \((C + G)/(A + T)\) is species-specific: in all cells of the body, the ratio \((C + G)/(A + T)\) is the same.

In bio systems, the functions of immune protection are implemented through
- internal mechanisms for rapid response to threats and destabilizing influences, distributed over the levels of the IPS hierarchy,
- long-term processes of life experience accumulation, which are of an evolutionary nature [18, 20].

Thus, the main features of the DNA code that provide information security and functional stability of bio systems can be reduced to the following: information redundancy and complementarity of coding, uniformity of mass distribution and balance of the system of connections across the DNA molecule.

Bio system analogy in the structure of protection of IT systems is based on the hierarchy of IPS, built-in mechanisms of immune protection and experience accumulation. Well-known IPS are usually limited to the implementation of the functions of the lower level of the protection system and the anti-virus orientation of the immune protection means. According to [19], about 70% of virus attacks are carried out from the outside via the entry point to the protected network and only about 30% from the inside. The first can be attributed to external threats to the life support of the system, the second - internal. In both cases, the immune defense of the bio system is activated. The implementation of the idea of information immune system is that in case of detection in a network of signs of infection send a sample of the new virus in anti-virus center, where, after some time, get virus

![Diagram of the DNA molecule.](image)
updates, which distribute over a corporate network before to spread the virus.

**Conclusion**

Thus the following conclusions can be drawn:

1. The analysis showed that the intrusion detection system is used to protect "information as an intellectual tool in which, as a rule, used a neural network system fuzzy logic and rule-based expert systems; what is needed to solve the individual tasks of information protection, and to develop a common approach to the use of intelligent tools for creating complex adaptive protection of IT systems on the basis of biology

2. Biological systems form a hierarchy of information systems with a unified approach to methods and methods of information transformation, storage and transfer, which have high security. The security of the bio system is provided by mechanisms of heredity and variability, which are informational in nature.

**References:**