ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 9 , September 2018

Classification of Modern Security Monitoring Systems in Computer Systems and Networks

Kadirov Mirhusan Mirpulatovich, Tojikhujaeva Nodirakhon Zakirovna, Kasimova Gulnora Ismoilovna

Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

Assistant, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: The article considers the classification of modern security monitoring systems in computer systems and networks. The classification of modern security monitoring systems is generalized. And also, the architecture of security monitoring systems is generalized. Performance indicators of security monitoring systems for modern security monitoring tools. Intrusion detection systems are analyzed.

KEYWORDS: monitoring systems, computer systems, networks, protection of information, threat, data processing, safety analysis, intrusion detection systems, classification of systems, resource control, principles of detection, detection of abnormal behavior, DBMS.

I. INTRODUCTION

In conditions of dynamic social transformations occurring in the world and accompanied by the rapid penetration of global computer networks into a huge number of areas of human activity, the task arises of automated processing of information in order to identify threats to information security arising from the operation of various systems.

Comparative ease of access to various resources of information and telecommunications systems makes it necessary to identify possible areas of information impact and attacks. The threats of confidentiality, integrity and accessibility of information are becoming especially urgent.

II. CLASSIFICATION OF SECURITY THREATS TO COMPUTER SYSTEMS AND NETWORKS

The protection of confidential and valuable information processed in computer networks from unauthorized access and modification is designed to provide a solution to one of the most important tasks of protecting the property rights of computer owners and users - the protection of property embodied in the information processed by computers against all possible malicious attempts that may inflict significant economic and other material and non-material damage[1].

All the set of potential threats by the nature of their occurrence is divided into two classes: natural (objective) and artificial (subjective). At the same time, artificial deliberate threats to the security of the computer systems and networks (CSN) can be characterized by such parameters as the nature of the crime, the type of implementation, the objectives pursued, the object of influence, the place of origin. In Figure 1 shows the classification of such threats.

Threat to the interests of the subjects of information relations is a potentially possible event, a process or phenomenon that, through exposure to information or other components of the CSN, can directly or indirectly lead to damage to the interests of these entities.

The vulnerability of the information system is any property (element) of the information system, the use of which by the violator can lead to the realization of the threat.

According to the classification of CSN vulnerabilities, their following types are distinguished [2, 3]:
- design vulnerability (when developing the CSN project);
- Implementation vulnerabilities (when implementing software or hardware CSN);
- Configuration vulnerabilities (incorrect management of CSN components by the administrator);
- Vulnerability of use (introduced by the user in the operation of the CSN).

A possible channel for information leakage is a method that allows an attacker or an intruder to gain access to information processed or stored in the CSN. In this case, the main type is the means by which this channel was used. In general, three types are distinguished: man, equipment, program.

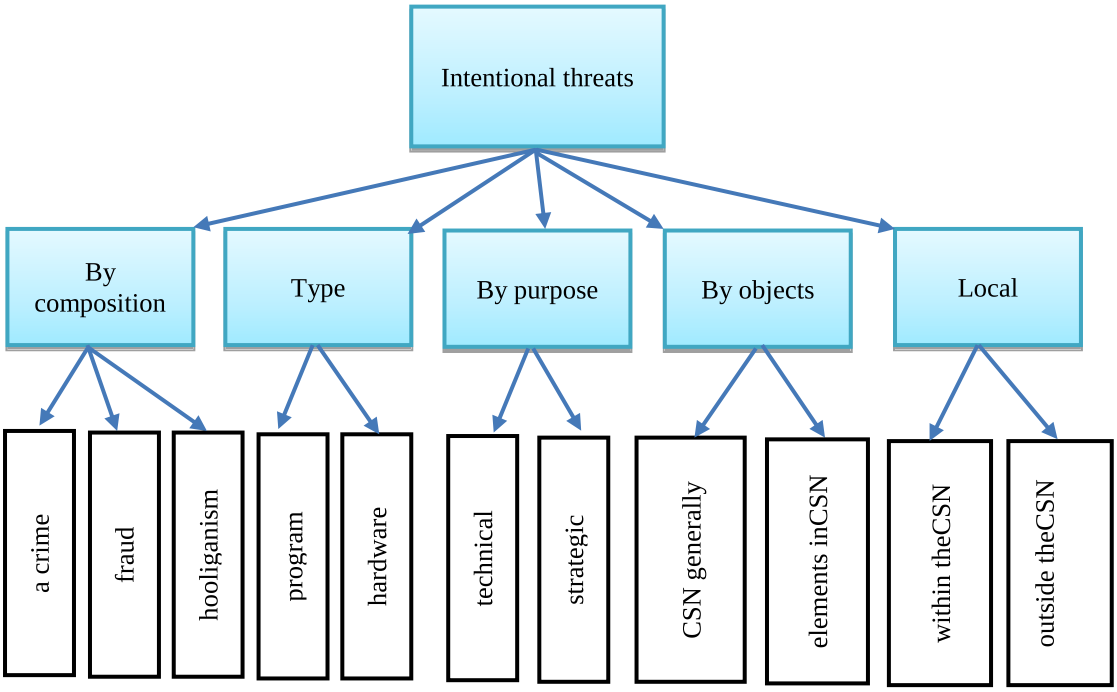

Figure 1. Classification of deliberate security threats to CSN.

III. GENERALIZED CLASSIFICATION OF MODERN SYSTEMS FOR MONITORING THE SECURITY OF COMPUTER SYSTEMS AND NETWORKS

Security monitoring is a set of measures and activities (organizational, technical and legal) aimed at monitoring, analyzing and forecasting the safety conditions of CSN [4]. The need to use security monitoring system(SMS) in the CSN is determined by the fact that the use of conventional means and mechanisms for protecting information that is processed is not sufficient, since they support only the basic functions of securing the system and do not allow monitoring the security of the operation of information systems.

Currently, the classification of security monitoring systems is presented in the form of three groups (Figure2), spaced along the principle of detection, scope and methods of detecting attacks [5].

According to the principle of detection, the following security monitoring systems are distinguished [2, 4, 6]:

1) Based on the detection of abnormal behavior - the process of detecting intrusion by comparing the actions of subjects with patterns of normal (normal) activity of legal subjects. Thus, if a model of the normal behavior of the subject in the system is established, then all other actions in the system are treated as an intrusion. The disadvantages of this approach include: abnormal actions that are not intrusions are considered as intrusions; Invasion actions that are not abnormal are not detected;

2) Based on the detection of abuse - the process of detecting an attack by comparing the current state of the monitored signs of actions of subjects with known characteristics of intrusions. In this case, already known types of

intrusion are recognized, and previously unknown invasions are not detected. The main task in building Abuse Detection Tools is to create a database with templates and signatures of all possible attacks.

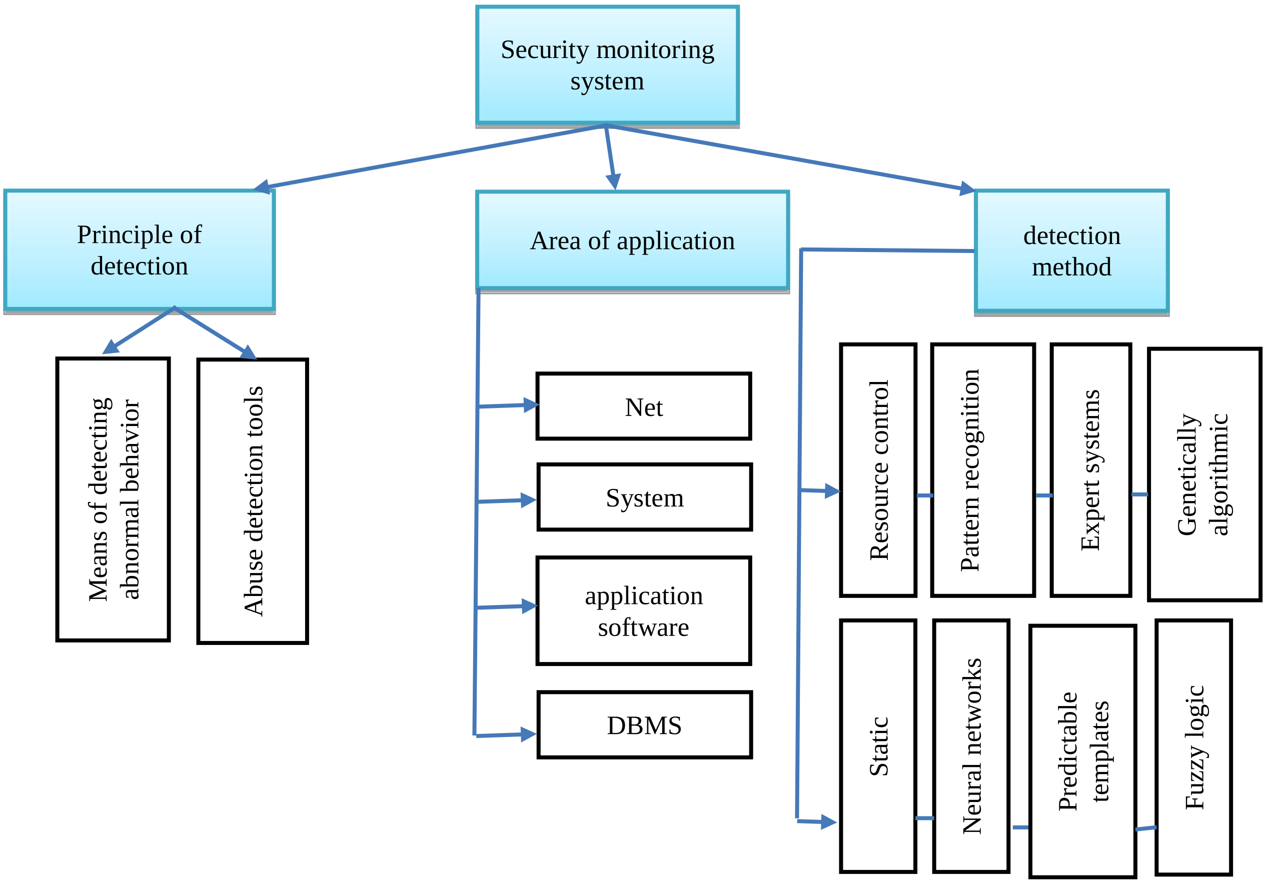

Figure 2. Classification of security monitoring systems CSN.

In the field of application of security monitoring systems, there are [2,7, 8]:

1) Intrusion detection systems at the network level, aimed at detecting attacks on the entire network or network segment. They function on specialized servers (capture and analyze packets) or are integrated into routers/switches (information that passes through these devices is analyzed);

2) Intrusion detection systems at the system level, recognizing attacks at the level of the operating system (OS) of workstations and servers. At the same time, as a rule, they work at the OS kernel level and operate with information presented in logs;

3) Intrusion detection systems at the application software level, which identify attacks on specific applications. These systems can analyze the logs of these applications or be integrated into them;

4) intrusion detection systems at the DBMS level, detecting attacks on specific database management systems.

The following security monitoring systems are distinguished according to methods for detecting extraordinary situations [9, 10]:

1) Based on statistical analysis, which accumulates statistical information about the actions of subjects, further compared with the indicators of normal behavior of legal subjects or, conversely, actions characteristic of the invasion;

2) Based on artificial neural networks that are trained in a special way to identify typical intrusion characteristics or statistically significant deviations from the normal mode of operation of subjects;

3) Based on the method of predictable generated patterns, which is based on the prediction of future events (system states) by analyzing what has already happened;

4) On methods based on the use of a fuzzy logic apparatus, implying the construction of a fuzzy set of behaviors of subjects or fuzzy rules for detecting abuses;

5) Based on the control of resources, which continuously monitors programs, files and other information resources for integrity and permissible operations with them;

6) Based on pattern recognition, in which all events in the CSN are compared with patterns of normal behavior of subjects or, conversely, abuses;

7) Based on the expert system, which makes decisions about the belonging of an event to the class of attacks based on the formed rules;

8) Based on control of transition states, when all actions in the system are considered as system transitions from one state to another, on the basis of which the conclusion is made about a possible intrusion of an attacker;

9) Based on deterministic finite automata using automaton mapping to form a conclusion about possible intrusions;

10) Based on a genetic algorithm that allows you to identify intrusions, using tools such as generation of offspring, mutation and selection of attacks.

Classical modern security monitoring system necessarily includes one component of all the three groups described above [5].

IV. GENERALIZED ARCHITECTURE OF SECURITY MONITORING SYSTEMS CSN

All CSN security monitoring systems can be divided into two categories: stand-alone and client-server systems [2, 11].

When using client-server systems, SMS agents (sensors, tracking modules) are installed at the most critical points of the network, which are responsible for detecting attacks and responding to them. All control is carried out from the center console, which also transmits all signals about emergency situations. In this case, the console may not contain modules that perform data sampling, analysis and response, so that in the event of damage to the console or communication channel, the PMS operation does not stop.

Single-level client-server systems usually function in small corporate networks (up to several tens of sensors), and the hierarchical scheme is used in case of complex network topology or geographic / functional disparity of the protected objects.

A model based on autonomous agents implies the presence of several small independent intrusion detection subsystems. Its advantages are: efficiency, noise immunity, resistance to degradation, extensibility and scalability. The shortcomings of the system include the need to monitor the interaction of modules with each other.

V. RESULT

Protection of confidential and valuable information processed in computer networks from unauthorized access is one of the most important tasks of information protection.

Consider the functioning of security monitoring systems:

1) The probability of a correct intrusion detection by a security monitoring system

$$P = 1 - \max\{1 - P_I, P_{II}\}, \tag{1}$$

where P_I and P_{II} the probabilities of errors of the first and second kind, respectively.

2) Redundant configuration of the information security system:

$$K_1 = \frac{m_1 - n_1}{n_1} \quad u \quad K_2 = \frac{m_2}{n_2} \tag{2}$$

Where K_1, K_2 - redundancy coefficients; m_1 -number of protection mechanisms; m_2 -number of security monitoring system agents; n_1 -minimum required number of protectors to ensure a given level of security, while $m_1 > n_1$; n_2 –amount of information resources.

3) Estimates of costs required for the implementation of safety monitoring systems.

Table 1. Performance indicators of security monitoring systems.

№	Name	Probability of correct detection*	Configuration redundancy**	Cost estimates ***
1	RealSecure	0.89	0,71	130
2	Open View	0.90	0,56	140
3	Tivoli	0.88	0,62	140
4	Enterprise Security	0.90	0,59	150

* - according to information from manufacturers websites and independent tests

** κ_1 -, according to information from manufacturers websites

*** - c.u./mon for protection of one resource (including cost of support and payment of the security administrator)

VI. CONCLUSION AND FUTURE WORK

Thus, it is important to create new methods, as well as modified security monitoring tools that provide a high probability of detection and timely warning of attacks by intruders.

Based on the analysis of problems arising from the functioning of security monitoring tools in modern computer systems and networks, the main focus of research is the development of methods and means of monitoring security that increase the effectiveness of security monitoring systems against the actions of intruders due to:

- predicting possible actions by intruders;
- dynamic analysis of the risks of the implementation of threats to the security of information resources;
- recommendations to the system of adaptive security management for migration/modification of protection when the level of threat is changed.

This work on the subject of the grant ЁОТ-Атех-2018-168“Improving methods and means of detecting attacks in computer networks”.

REFERENCES

[1] Kadirov M.M., TulyaganovZ.Ya., Karimova N.A., Comparative analysis of modern security monitoring systems. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 8, India 2018, p. 6548-6553.

[2] Лукацкий А.В. Обнаружение атак. -СПб.:‖БХВ-Петербург‖, 2003. - 608с.

[3] Mukhin V.E., Volokita A.N., Pavlenko E.N. Monitoring of information resource states for the implementation of adaptive management of the security of computer systems. //Artificial Intelligence. N 3, 2006. - с. 773 - 782.

[4] Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-К.: «ТИДДС», 2001. 688 с.

[5] Mukhin V.E., Volokita A.N. Integrated security monitoring system based on the analysis of the objectives of the actions of subjects of computer systems and networks. // Control systems and machines. №5, 2006, -p.85-94.

[6] RehmanRafeeq. Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID. - Prentice Hall PTR, 2003 -288p.

[7] Mukhin V. Ye., Shyrotchin V.P. Network scanners as security monitoring means in the computer systems //Proc. of International Symposium on Signal, Circuits and Svstems (SCS'2001), Iasi, Romania, July 10-11, 2001. - pp. 144-147.

[8] Santi Paolo. Topology Control in Wireless Ad Hoc and Sensor Networks – Wiley, 2005 – 280p.

[9] Axelsson Stefan, Sands David. Understanding Intrusion Detection through Visualization (Advances in Information Security), - Springer, 2005 – 145p.

[10] Proctor Paul. Practical Intrusion Detection Handbook. Prentice Hall, 2001.

[11] Rajaboevich G. S., Mirpulatovich K. M., Yakubdjanovich T. Z. The Methodology of the Ways for Increasing the Efficiency of Intrusion Detection Systems //International Journal of Engineering Innovations and Research. – 2016. – Т. 5. – №. 5. – С. 296.

AUTHOR'S BIOGRAPHY

Kadirov Mirhusan Mirpulatovich. Assistant professor.
Was born May22, 1985 year in Tashkent city, Republic of Uzbekistan.
Has more than 80 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

Tojikhujaeva Nodirakhon Zakirovna. Senior Lecturer.
Was born February14, 1977 year in Tashkent city, Republic of Uzbekistan. Has more than 18 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

Kasimova Gulnora Ismoilovna, Assistant.
was born May30, 1989 year in Tashkent city, Republic of Uzbekistan.Has more than 10 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.