ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 8 , August 2018

Comparative Analysis of Modern Security Monitoring Systems

Kadirov Mirhusan Mirpulatovich, Tulyaganov Zoxidjon Yakubdjanovich, Karimova Nazimakhan Aybekovna

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

ABSTRACT: The article makes a comparative analysis of methods and means of monitoring security in computer systems and networks. Threats and security risks in modern computer systems and networks are considered. And also in the article the classification according to the principle of construction and area of application of modern software and hardware monitoring and safety analysis.

KEYWORDS: monitoring systems, computer systems, networks, protection of information, threat, software and hardware monitoring tools, data processing, safety analysis, intrusion detection systems, VPN, VPN server, CSN.

I. INTRODUCTION

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. To it adjoins the task of protecting state secrets, where the state acts as the owner of information.

The threat, in general, is understood to be a potential event, action (action), process or phenomenon that can lead to damage to someone's interests [1]. 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 computer systems and networks (CSN), can directly or indirectly lead to damage to the interests of these entities. The ability to implement threats depends on the presence of vulnerabilities in the CSN, the number and specifics of which are determined by the type of tasks to be performed, the nature of the information being processed, the hardware and software features of the system, the availability of protection equipment and their characteristics [2]. 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 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.

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.

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.

II. MODERN TOOLS FOR MONITORING THE SECURITY OF COMPUTER SYSTEMS AND NETWORKS

The main criteria for selecting and using a specific security monitoring tool are the goals and objectives of ensuring the protection of information processed by CSN. At the same time, first of all it is determined: from what

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 8 , August 2018

threats it is supposed to build defense, what means can be used to prevent these threats, and what measures have already been used for the purposes of protection [3].

In Table. 1 provides a classification by the principle of construction and application of modern software and hardware security monitoring and analysis of firms-developers of different countries used to ensure safe processing of data in the CSN [4,5, 6].

Table 1
Modern means of monitoring and analysis of safety CSN

The principle of constructing a tool and scope	Name of the facility (manufacturer)
Systems of monitoring and analysis of safety CSN	Systems Management Server (MS), Enterprise Security Manager (Symantec), Novell Sentinel (Novell), Open View (HP), Identity Management Services (IBM), Netforensics SIM/Cisco SIMS (Cisco), Kane Security (Intrusion Detection), TopS BI (TopS BI), Smart Management (Check Point), Condor, Digital Security, Operations Manager Server (MS), Tivoli Express (IBM), Kaspersky Total Space Security (Kaspersky Lab);
Integrated Intrusion Detection Systems	RealSecure (ISS), Cisco IDS / IPS (Service module, Network module), Statistica Neural Networks, Identity Risk and Identification Solution (IBM), Equant Managed IDS, Outpost (RNT), Security Suite SBE (Sophos),Security Forse (HP);
Workstation event analysis tools	WMI (MS), VMM (MS), InterSpect (Check Point), Integrity Security Client (Check Point), PortalProtect (Trend Micro), Cisco Security Agent (Cisco), Notification Services (MS), Client Policy Manager (Websense), Integration
Network Security Monitoring Tools	Cisco Guard and Traffic anomaly detector (Cisco), Network VirusWall (Trend Micro), Distributed Wireless Security Auditor (IBM), SessionWall, (AbirNET), ISA Server 2004 (MS), PC-Duo (Vector Networks Group), Snort, Safe 'n'Sec Business (StarForce), eTrust ID, NetRanger, NetProwler, BlackICE Sentry, SecureNetPro, CyberCop Monitor, LANguard, OpenSnort, Shadow, Network Security Agent; Outpost Network Security (Agnitum Ltd);
Tools for monitoring virtual secure networks VPN	ISA Server 2004 (MS), CiscoWorks2000 VPN / Security Management Solution (Cisco), Equant Managed Crypto VPN (Equant), Jet Trail (Jet Infosystems);
Means of detecting attempts of unauthorized access and management of security policy	Intruder Alert (Symantec), Equant Secure Authentication (Equant), DeviceLock, Cisco Secure Policy Manager (Cisco);
DBMS and application monitoring systems	SQL Trace (MS), Cerberus (Sats Technologies), SKL Server Management Studio (MS), PerfMon (MS);
Security analysis tools	Internet Scanner (ISS), Baseline Security Analyzer (MS), SATAN, Equant Managed Active Audit (Equant), Threat Watcher (Websense), Microsoft Security Assessment Tool (MS), Xspider (Positive Technologies).

In general, the CSN security monitoring and analysis systems allow you to collect and analyze information from various components of the security system (firewalls, intrusion detection systems, routers, VPN servers, operating systems, DBMS, antivirus, etc.). Then, based on the correlation analysis of events, threats are detected and the process of resolving arising incidents is tracked [7]. In addition, some manufacturers prefer not to produce complex solutions,

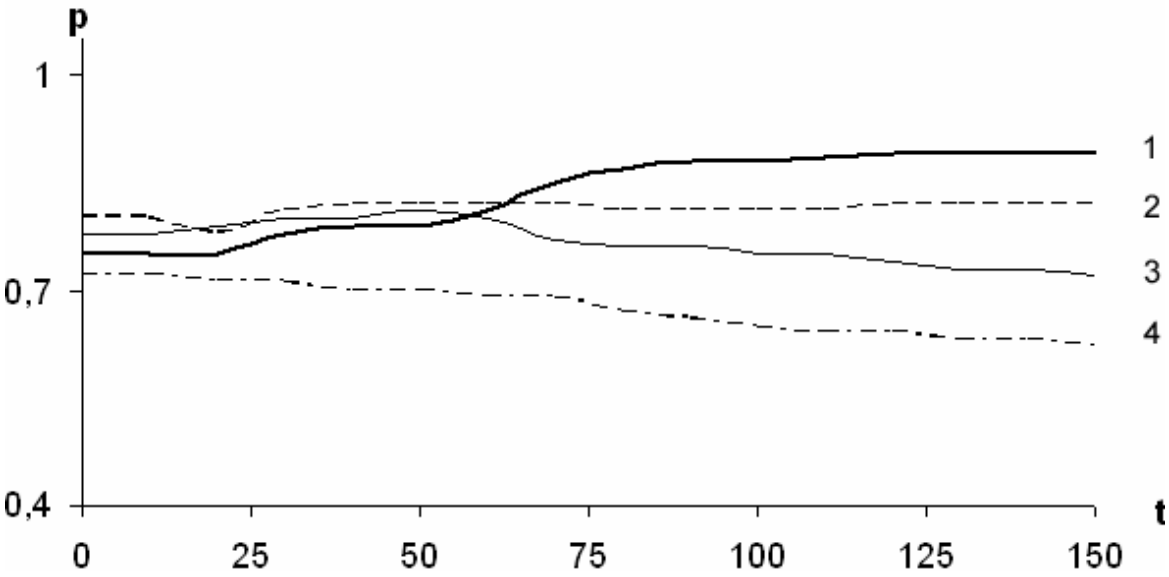
ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 8 , August 2018

but monitoring and analysis tools aimed at identifying and analyzing extraordinary situations in specific CSN components.

The existing security monitoring tools developed by manufacturers are generally "closed" to users and cannot be modified to the requirements of specific institutions, corporations and possible special conditions for their use, which raises the problem of developing new protection and analysis tools with the possibility of their target adaptation [8]. This problem requires the creation of models and tools for modeling and verification of developed and applied protection. When developing mechanisms and means of protection, it is necessary to take into account existing security threats in the CSN.

III. COMPARATIVE ANALYSIS OF SECURITY MONITORING SYSTEMS USING THE METHOD OF ANALYSIS OF EXTRAORDINARY EVENTS

In figure. 1 depicts the relative dependencies of the intrusion detection probabilities (p) on time (t) for different SMS. Over time, the effectiveness, defined as the probability of intrusion detection, for some media (neural networks, fuzzy logic) increases, and for others (expert systems, static systems for detecting abnormal behavior (SSDAB)) falls [9].



1 - neural networks
2 - expert systems
3 - fuzzy logic
4 - statistical SDAB

Figure 1. Comparative dependencies of probabilities (p) of intrusion detection on time (t) for various intrusion detection means intruders

As can be seen from figure 1, neural networks show the best dynamics of the development of the required characteristic (p), resulting from the learning of the neural network. In this case, the coefficients of the neural network are its internal characteristic, and cannot practically be analyzed.

Expert systems are a little less effective and require manual adjustment, but they can present the entire process of proving the result. Systems based on fuzzy logic and statistical SDAB show similar results, explained by the internal similarity of implementation.

In figure 2 is a diagram of the interaction between the security tools of the CSN, where the safety monitoring system rises to the same level as the CSN security management tools.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 8 , August 2018

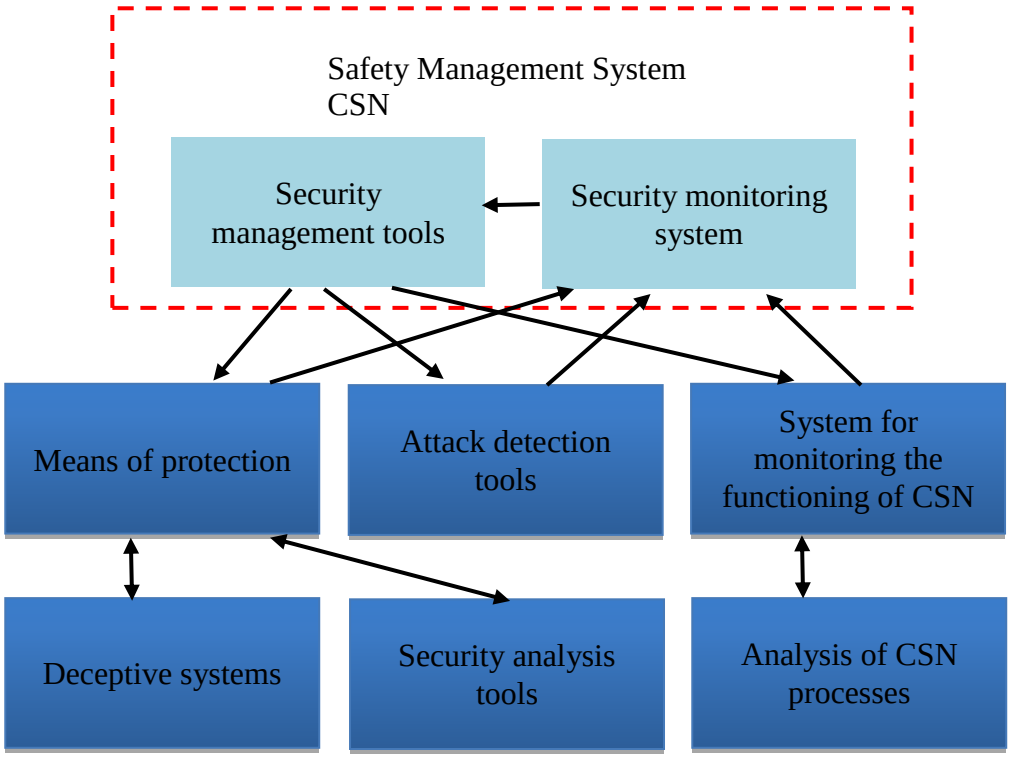


Figure 2. One-level security management scheme CSN

Under the system of security monitoring in its classical view means means of detecting attacks (invasions). But, taking into account the shortcomings of this approach shown below, it is more advisable to raise the security monitoring system of the CSN one level with security management tools. At the same time SMB receives information from security equipment, intrusion detection means and monitoring systems of CSN functioning. In addition, SMS are able to analyze data from fraudulent systems, security analysis tools and analyzers of processes taking place in the CSN. Thus, SMS allow building an integral picture of the actions of intruders and making correct decisions on further countermeasures in their relation.

IV. RESULT

The File System Viewer (HP Open View) scans the file system and produces reports on the age of the files, their size, type and frequency of user access to them, from which you can decide the behavior of users. The Chargeback, Report Designer and Global Reporter utilities are designed for billing for storage, reporting, and aggregating reports from multiple Storage Essentials.

In addition, the analysis of access to network resources can help identify the attacks directed at them (a fragment of the TCPdump log):

07: 11: 38.123565 200.0.0.200> 200.0.0.34: icmp: echo request
07: 11: 51.456342 200.0.0.200> 200.0.0.47: icmp: echo request
07: 11: 04.678432 200.0.0.200> 200.0.0.3: icmp: echo request
07: 12: 18.985667 200.0.0.200> 200.0.0.12: icmp: echo request
07: 12: 31.024657 200.0.0.200> 200.0.0.11: icmp: echo request
07: 12: 44.044567 200.0.0.200> 200.0.0.9: icmp: echo request

Analysis and testing of network / hosts for bandwidth / vulnerable areas, selective testing - the process of detecting vulnerabilities in the KCC. Analysis of security is the search and analysis of vulnerabilities in the network, which is carried out using scanning and probing mechanisms.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 5, Issue 8 , August 2018

Table 2.
Analysis of the network to vulnerable areas using the Symantec Enterprise Security software module.

Risk	Port	Network resource	HostName	Service	Vulnerability
1	22	10.1.6.3	S01	OpenSSH	No
1	25	10.1.6.3	S01	Exim smtpd	No
2	53	10.1.6.3	S01	ISC Bind	XSS
3	8009	10.1.6.4	Srv1	jakarta-tomcat	DoS

Security reliability testing systems examine the CSN for potential vulnerabilities therein, generalize this information, and generate reports.

Predicting possible actions of intruders based on the analysis of goals is an attempt to construct a model of the behavior of the offender in order to predict its possible actions to ensure a given level of security of resources. To date, existing tools do not predict the possible next step of the subject, but only take into account expert estimates.

V. CONCLUSION

Based on the analysis of problems arising from the functioning of security monitoring tools in modern computer systems and networks, the main direction of research is identified - to increase the effectiveness of the security monitoring systems by predicting the targets of attackers and preemptive reaction to their actions; Dynamic analysis of the risks of carrying out NDS taking into account the value of information resources; recommendations on reconfiguration/modification of protective equipment, taking into account changes in the level of risks.

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

REFERENCES

[1] Беляев А., Петренко С. Системы обнаружения аномалий: новые идеи в защите информации.// Экспресс-Электроника, №2, 2004. – с. 49 – 54.

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

[3] Stephen Northcutt. Network Intrusion Detection. An Analyst's Handbook (2 Edition). New Riders Publishing. 2000.

[4] Wilding Edward. Information Risk And Security: Preventing And Investigating Workplace Computer Crime - Gower Publishing Company, 2006 – 350p.

[5] Phoha Shashi, La Porta Thomas, Griffin Christopher. Sensor Network Operations - Wiley-IEEE Press, 2006 – 724p.

[6] Holden Greg. Guide to Firewalls and Network Security: Intrusion Detection and VPNs - Course Technology, 2003 – 512p.

[7] Sagatov M., Irgasheva D., Mirhusan K. Construction Hardware Protection Infocommunication Systems from Network Attacks //Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE). – International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE), 2015. – С. 271.

[8] 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.

[9] 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.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 5, Issue 8 , August 2018

Kadirov Mirhusan Mirpulatovich Assistant professor. 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.

Tulyaganov Zoxidjon Yakubdjanovich Assistant. 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.

Karimova NazimakhanAybekovna, Senior Lecturer. Has more than 15 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.