Chemical Technology, Control and Management

Volume 2021 | Issue 3 Article 8

6-28-2021

ISSUES IN FUNCTIONING EFFICIENCY OF SECURITY MONITORING SYSTEMS IN INFOCOMMUNICATION SYSTEMS

Majid Karimov Malikovich
Cabinet of Ministers of the Republic of Uzbekistan State Testing Center, Address: 12 Bogishamol st., 100084, Tashkent city, Republic of Uzbekistan, E – mail: mmkarimov@list.ru;, mmkarimov@list.ru

Sevara Khamdamova Mirazizovna
Tashkent State Technical University, Address: 2 Universitetskaya st., 100095, Tashkent city, Republic of Uzbekistan E – mail: mssagatova@mail.ru., mssagatova@mail.ru

ISSUES IN FUNCTIONING EFFICIENCY OF SECURITY MONITORING SYSTEMS IN INFOCOMMUNICATION SYSTEMS

Erratum

there was a small change

ISSN 1815-4840, E-ISSN 2181-1105
Himičeskaâ tehnologiâ. Kontrolʹ i upravlenie
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2021, №3 (99) pp.66-72. https://doi.org/10.51346/tstu-02.21.3-77-0022
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm/
Since 2005

ISSUES IN FUNCTIONING EFFICIENCY OF SECURITY MONITORING SYSTEMS IN INFOCOMMUNICATION SYSTEMS

Karimov Majid Malikovich[1], Khamdamova Sevara Mirazizovna[2]

[1]Cabinet of Ministers of the Republic of Uzbekistan State Testing Center,
Address: 12 Bogishamol st., 100084, Tashkent city, Republic of Uzbekistan,
E – mail: mmkarimov@list.ru;
[2]Tashkent State Technical University, Address: 2 Universitetskaya st., 100095, Tashkent city, Republic of Uzbekistan
E – mail: mssagatova@mail.ru.

Abstract. *The security monitoring system (SMS) receives information from the means of protection, detecting attacks, systems for monitoring the functioning of information communication systems (ICS) and performs adaptive security management of ICS, providing a flexible response of the security system to the actions of the intruder. In this case, the result of the functioning of the SMB are recommendations for modifying the ICS security system, in accordance with the specified restrictions, in order to minimize the possible damage from the implementation of threats. A complex of security systems is used in modern ICS. Typically, different systems are not linked and are purchased from different manufacturers. Even when using protection systems from one manufacturer, it is quite difficult to understand the events taking place in the ICS. When assessing the effectiveness of SMB, methods of expert assessments are used, i.e. methods of organizing work with specialist experts and processing expert opinions expressed in quantitative and / or qualitative form in order to prepare information for the formation of internal characteristics of the ICS SMB. Based on the analysis of existing approaches to assessing the effectiveness of SMB in the work for conducting research on the parameters of SMB in the ICS, a method is proposed that allows to evaluate the efficiency of SMB functioning.*

Keywords: *security monitoring system, infocommunication systems, vulnerability, attack detection tools, expert assessment methods, security management.*

Аннотация. *Хавфсизлик мониторинги тизими (ХМТ) маълумотни ҳимоялаш воситалари, хужумларни аниқлаш воситалари, ахборот коммуникация тизимларни (АКТ) ишлаш мониторниги тизимларидан олиб бузғунчининг харакатларига хавфсизлик тизимни мослашувчан реакциясини таъминлаб АКТ химояланишиини адабтив бошқаришини амалга оширади. Бунда ХМТ ни ишлаш натижаси бўлиб берилган чекловларга мос равишда тахдидларни амалга оширилишидан эҳтимолий зарарни минималлаштириш учун АКТ хавфсизлик тизимини модификациялаш бўйича тавсиялари хисобланади. Замонавий АКТларда хавфсизлик тизимларининг комплексидан фойдаланилади. Одатда турли тизимлар бир бири билан боғлиқ бўлмасдан турли ишлаб чиқарувчилардан ҳарид қилинган. Ҳатто бир ишлаб чиқарувчининг ҳимоя тизимларидан фойдаланилган холда ҳам АКТ да содир бўладиган ҳодисаларни текшириш мураккабдир. ХМТ нинг самарадорлигини бахолашда эксперт баҳолаш усулларидан, яъни АКТ ХМТ ички характеристикаларини шакллантириш маълумотларни тайёрлаш мақсадида миқдорий ва сифат шаклида ифодаланган, мутахассис экспертларни ишини ташкил қилиш ва эксперт фикрларини қайта ишлаш усулларидан фойдаланилади. ҲМТ самарадорлигини баҳолашнинг мавжуд ёндашувларнинг тахлили асосида ишда АКТ даги ХМТ параметрларини ўрганиш учун ҲМТ ишлаш самарадорлигини баҳолаш имкониятини берадиган методика таклиф этилган.*

Таянч сўзлар: *хавфсизлик мониторинги тизими, инфокоммуникация тизимлари, заифлик, хужумларни аниқлаш воситалари, эксперт баҳолаш усуллари, хавфсизликни бошқариш.*

Аннотация. *Система мониторинга безопасности (СМБ) получает информацию от средств защиты, средств обнаружения атак, систем мониторинга функционирования инфокоммуникационных систем (ИКС) и выполняет адаптивное управление защищенностью ИКС, обеспечивая гибкую реакцию системы безопасности на действия нарушителя. При этом результатом функционирования СМБ являются рекомендации по модификации системы безопасности ИКС, в соответствии с заданными ограничениями, для минимизации возможного ущерба от реализации угроз. В современных ИКС используется комплекс систем безопасности. Как правило, различные системы не связаны между собой и приобретены у различных производителей. Даже при использовании систем защиты одного производителя, достаточно сложно разобраться в происходящих в ИКС событиях. При оценке*

эффективности СМБ используются методы экспертных оценок, т.е. методы организации работы со специалистами-экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для формирования внутренних характеристик СМБ ИКС. На основании анализа существующих подходов к оценке эффективности СМБ в работе для проведения исследований параметров СМБ в ИКС предложена методика, позволяющая оценивать эффективность функционирования СМБ.

Ключевые слова: *система мониторинга безопасности, инфокоммуникационные системы, уязвимость, средства обнаружения атак, методы экспертных оценок, управление безопасностью.*

Introduction

The requirements for the security of modern infocommunication systems (ICS) imply an assessment of the effectiveness of protection. Safety monitoring is actions aimed at monitoring, analyzing and predicting the safety states of complex systems. Analysis of existing security monitoring systems (SMS) shows the need to conduct a comprehensive assessment of the actions of attackers, building a chain of implemented vulnerabilities, determining the ultimate goal of their actions and assessing the security risks of information resources.

The development of new methods, as well as modified security monitoring tools that provide a high probability of correct detection and timely prevention of malicious attacks is an urgent task. To analyze the characteristics of the created ICS security monitoring tools, it is necessary to develop specialized software environments that implement modeling and assessment of the compliance of the characteristics with the requirements of these information protection mechanisms.

Based on the analysis of the problems arising in the development of security monitoring tools in modern ICS, the following aspects are highlighted: the formation of analytical assessments of the parameters of the SMS in ICS, the development of new methods for assessing the level of intrusion threats and methods for analyzing the risks of the implementation of threats to the security of information resources, adaptive management of ICS security, providing an increase in the efficiency of SMS, development of specialized tools for modeling and analysis of SMS in ICS.

A complex of security systems is used in modern ICS. Typically, the various systems are not interconnected and are purchased from different manufacturers. Even when using protection systems from one manufacturer, it is quite difficult to understand the events taking place in the ICS. At the same time, the administrator works with several management and monitoring consoles at once, which require constant attention and high qualifications for a quick response to security events. If a security incident occurs in the ICS (in the case of an unauthorized system), then the administrator needs to compare the information supplied not only by security tools, but also by specific application systems, for example, databases or a www-server. As a result, the administrator is unable to analyze everything that happens in the ICS and cannot correctly respond to security incidents [1,2,3,4].

Research Methods and the Received Results

In the process of managing and solving ICS security problems, the question of collecting information about events occurring in ICS, as well as its analysis, often arises. At the same time, it is desirable that the information collection system comply with a number of requirements for control systems. These requirements are defined by international standards that summarize the experience of using control systems in various fields, which divide the tasks of the control system into five functional groups [5,6,7,8]: network configuration and naming management, error handling, performance and reliability analysis, security management , network accounting.

With regard to the collection of statistical information about events in the ICS and occurring emergency situations, the following groups are responsible for performing such tasks:

Management of network configuration and naming (Configuration Management) - determination of network addresses, identifiers (names), geographic location, checking the correct operation of switches and routers.

Error handling *(Fault Management)* - identification, determination and elimination of the consequences of failures and failures in the work of ICS. In this case, not only registration of error messages is performed, but also their filtering and analysis based on a certain correlation model.

Performance and reliability analysis *(Performance Management)* - the accumulation of statistical information on the system response time, processor utilization rate, page interrupt rate, physical memory utilization rate, transaction rate, communication channel bandwidth between network subscribers, traffic intensity in individual network segments and channels, the probability of data corruption during their transmission, as well as the availability of the network or its specific transport service.

Security management - control of access to ICS resources (data and equipment), preservation of data integrity during storage and transmission, information on authentication and authorization of subjects and encryption.

Accounting for network and host activity *(Accounting Management)* - recording the time of use of various network resources (devices, channels and transport services).

To solve the problems described above, various software and / or hardware tools are used. A classic example of such a tool for a computer network is protocol analyzers, which allow you to do the following:

- to identify the most active senders (recipients) of data, as well as senders of broadcast packets;
- analyze erroneous packets by error type and packet source;
- collect information about collisions;
- to test the network for throughput by simulating the increased traffic level using the packet generation method;
- to identify the most vulnerable parts of the network in terms of the possibility of organizing attacks on availability;
- carry out selective testing of bridges and routers;
- perform a detailed analysis of the network topology, including hosts, routers, remote segments, and also identify duplicate addresses (possible connections of intruders);
- collect statistical data on the frequency of access to specific files and resources, information on sources and recipients of packets.

To minimize the information coming from various information security tools, ICS SMS are used, which also perform a primary check of the relationship of security events (Figure 1).

SMSs allow you to receive many (up to several million records) of events related to unauthorized actions from various network and system sources, to carry out their automatic processing, based on the rules set by the security administrator, taking into account the temporal characteristics of the events. As a result, several dozen real security events appear on the administrator console, which would take a long time to find.

SMS receives data from various network and system security tools, such as firewalls, intrusion detection tools, security analysis tools for OS and application systems, etc.

Minimization, establishment of interconnection, and prioritization of SMS information can significantly increase the efficiency of personnel responsible for information security, as well as provide a single, unified monitoring interface for heterogeneous means of protection.

SMS ICS are classified according to the areas of information infrastructure in which violations of the security policy are detected. At the same time, SMSs are allocated, focused on: a workstation, applications, database management systems (DBMS) and a computer network.

SMS workstations run on the protected node and monitor various security events, collect and analyze information reflecting the activity taking place in the operating system of an individual computer. This information is presented in the form of logs of the operating system and network traffic passing through the node.

Events entering the SMS log are compared with a signature database or normal operation profile using special algorithms that can vary depending on the implementation of the intrusion detection system. Suspicious events are classified, ranked, and notified to the administrator. Sometimes SMSs of this level control the activities of users in an on-line temporary mode, but this mechanism is implemented quite rarely [9,10,11,12,13].

SMSs at the application and DBMS level collect and analyze information from specific applications, for example, Web servers, firewalls or DBMS, and can be implemented in two ways. In the first case, they analyze the log records of a specific application or DBMS. The advantage of this solution lies in the simplicity of implementation and support of almost any application software and DBMS that record events in the log. However, for such a system to work effectively, it must be configured for a specific application, since most of them have a unique log format. The second way to implement systems of this level is to integrate them into a specific application or DBMS. At the same time, they become less universal, but more functional due to their close connection with the controlled software [2,14,15].

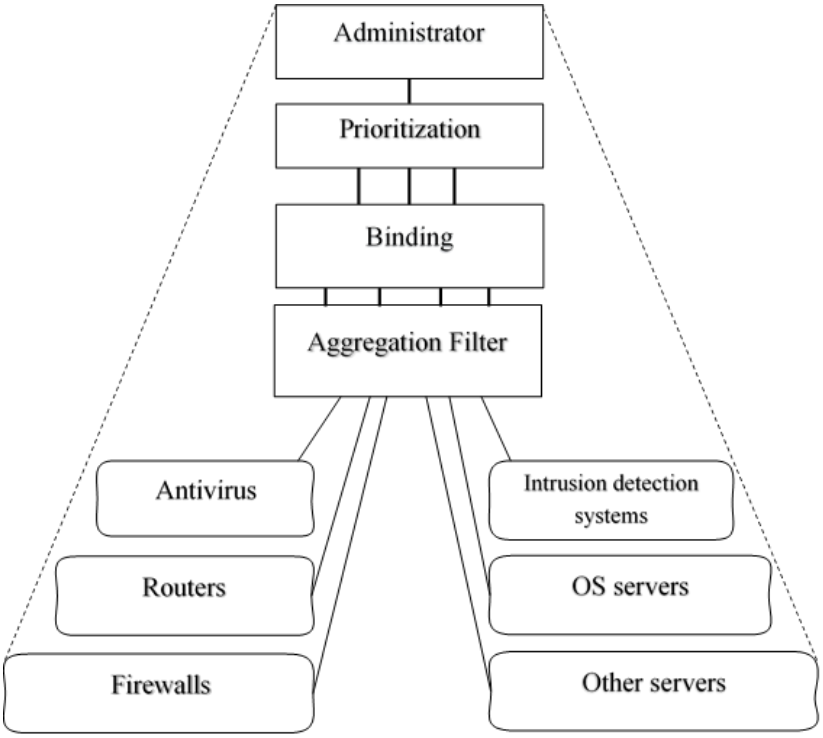

Figure 1. ***Minimization and analysis of information by the ICS security monitoring system.***

Network-level SMSs collect information from network traffic. They can be performed on ordinary or specialized computers, as well as integrated into routers or switches. In the first two cases, the analyzed information is collected by capturing and analyzing packets, while accessing network interfaces is carried out in promiscuous mode [2,8,16,17].

The SMS at the network level has access to all data transmitted between the ICS nodes. Since the SMS is performed on a computer (router) different from the monitored nodes, the efficiency of the latter does not decrease.

Expert assessment methods are methods of organizing work with expert experts and processing expert opinions expressed in quantitative and / or qualitative form in order to prepare information for the formation of internal characteristics of the ICS SMS.

The following stages of the examination are distinguished:

1) formation of an expert group;

2) planning and carrying out an examination;

3) analysis and interpretation of the results obtained.

Before the examination, the coefficients of authority (the degree of the expert's competence) are calculated - a number showing the weight with which the assessments of this expert are included in the statistical processing. The credibility coefficients are determined on the basis of the statistics of previous examinations or according to the results of the current examination [16,18].

Then the actual expert survey is carried out, which can be built according to one of the following principles [19]:

- Ranking methods (pairwise comparison) - experts need to choose the most significant of the two factors or build a priority chain of factors;
- Ball methods - an expert assigns a certain quantitative characteristic to each proposed factor, on the basis of which further analysis is made.

At the end of the expert survey, the degree of agreement of experts' opinions is assessed. If this value is outside the established limits, then the experts should check their judgments and "smooth out" the inconsistencies in the data.

Results and Discussion

To carry out studies of the parameters of the SMS in the ICS, a method has been developed that allows one to assess the efficiency of the SMS functioning.

In general, all actions of subjects in ICS, in the context of information security, can be classified as follows:

- permitted (normal) behavior of subjects;
- intrusions (internal and external) by violators.

Let $\boldsymbol{I}$ be the set of possible attacks on the ICS, $\boldsymbol{O}$ the set of normal profiles of the subjects' behavior. Let us designate: $m \in \{I\}$ - the set of intrusions that were not detected by the SMS, $f \in \{O\}$ - the set of normal behavior profiles of the subjects that were falsely identified by the SMS as intrusions.

Intrusion detection probability is calculated as:

$$P_n = 1 - \frac{m}{I} = 1 - P_I \quad (1)$$

where P_I is the probability of a type I error (lack of response to an attack).

The probability of false identification of normal behavior profiles of subjects is calculated as intrusion is:

$$P_f = \frac{f}{I-m+f} = P_{II} \quad (2)$$

where $I - m + f$ is the number of attacks detected by SMS, P_{II} is the probability of a type II error (false alarm)

In this case, the probability of correct detection of intrusions by SMS is calculated as:

$$P = 1 - \max\{1 - P_m, P_f\} = 1 - \max\left\{\frac{m}{I}, \frac{f}{I-m+f}\right\} = 1 - \max(P_I, P_{II}) \quad (3)$$

The resulting indicator is used for a comprehensive assessment of the effectiveness of the functioning of the SMS in the ICS.

To assess the effectiveness of the functioning of the adaptive control algorithm of the proposed SMS in the ICS, a parameter is used that determines the redundancy of the configuration of the information security system.

Let μ_i be the current security level of the *i – th* resource, $\alpha \le \mu_i < 1$, where α is the minimum security level set for this system, and, as mentioned above,r_i is the required security level of the *i – th* information resource, reduced to the range values $\alpha \le r_i < 1$, and established on the basis of indicators of the value of the information resource.

Let us introduce the indicator η of the redundancy of the configuration of the information security system for the *i – th* resource, calculated as:

$$\eta_i = |\mu_i - r_i| \quad (4)$$

Then the total indicator of redundancy of the configuration of the information security system is calculated as:

$$\eta = \sum_i \eta_i$$

To simplify this indicator, let us assume that the value of μ_i is determined only by the required amount of protective equipment.

Then the redundancy of the configuration of the information security system:

$$\eta_i = K_i = \frac{m_i - n_i}{n_i} \quad (5)$$

m_i is the number of protection mechanisms for the *i – th* resource; n_i is the minimum required number of security means to ensure a given level of security, while we assume that $m_i > n_i$;

Redundancy of the configuration of the protection system is considered as the excess of the current level of security over the required at the moment.

The obtained indicator of the redundancy of the configuration of the information security system is used for a comprehensive assessment of the effectiveness of the functioning of the SMS in the ICS.

Further, the estimates of the costs required for the implementation of SMS of the above types are carried out. When calculating the costs of building a SMS, the following factors are taken into account:

Z is the total cost, which is estimated as:

$$Z = z_1 + z_2 + z_3 + z_4 + z_5 + z_6 + z_7 \quad (6)$$

Where: z_1 – is the cost of the hardware part of the information collection agents; z_2 – costs for implementation and support of software (means of collecting information and checking the state of the CS); z_3 – costs of SMS; z_4 – is the cost of remuneration of experts; z_5 – is the cost of salaries of the security administrator; z_6 – the amount of computational costs required by SMS ICS; z_7 – costs due to missed attacks (loss, theft, distortion, unavailability of information, etc.).

To obtain a total estimate of the costs of implementing SMSs for the entire observation period, the obtained curves are integrated:

$$Z_\Sigma = \int_0^T z(t)dt \quad (7)$$

where $z(t)$ is the cost at a certain point in time, Z_Σ is the total cost of expenses for the entire observation period T.

The resulting indicator of total costs is used for a comprehensive assessment of the effectiveness of the functioning of the SMS in the ICS.

The probability of correct operation of the SMS is defined as:

$$P = 1 - \max\{P_I, P_{II}\} \quad (8)$$

where P_I is the probability of a type I error (no response to an attack), P_{II} is the probability of a type II error (false alarm).

Next, we introduce the concept of verifying decisions n, which shows the degree of correctness of decisions made by a security administrator or proposed decision support systems. This indicator is calculated as:

$$v = m / \sum_{i=1}^{n} k_i \quad (9)$$

where n is the total number of information resources, k_i is the number of decisions made for the *i* resource, m is the total number of correct decisions for all resources. The indicator *m* is determined by experts on the basis of an analysis of the situation that has developed after a decision has been made after a certain time interval.

Conclusion

Thus, taking into account the selected methodology for conducting examinations in determining the parameters of SMS, the specifics of their practical application, and using a set of

indicators, such as: the probability of correct detection of intrusions using SMS, redundancy of the configuration of the information security system, an estimate of the costs required for the implementation of SMS, verification of solutions adopted by the security administrator, based on the data of the SMS, the developed methodology allows to carry out research of the parameters of the security monitoring systems and allows to evaluate the efficiency of the SMS functioning in the ICS.

References

1. O.I.Sheluxin, D.J.Sakalema, A.S.Filinova, *Obnarujeniye vtorjeniy v kompyuterniye seti (seteviye anomalii) [Detection of computer network intrusions (network anomalies)]*. Moskva: Goryachaya liniya – Telekom, 2018, 220 p. (in Russian).
2. A.V.Lukatskiy, *Obnaruzheniye atak [Detecting attacks]*. Sankt-Peterburg: BKHV-Peterburg, 2003, 608 p. (in Russian).
3. Nil Dzh.Rubenking, “Kompleksy bezopasnosti” [Security complexes], *PC Magazine (Russian edition)*, no. 7, pp. 71-86, 2005. (in Russian).
4. Computer Crime and Security Survey, vol. V11I, no. 1. Spring 2002, Computer Security Institute. Federal Bureau Investigation's Computer Intrusion Squad.
5. V.F.Shan'gin, *Informatsionnaya bezopasnost' komp'yuternykh sistem i setey [Information security of computer systems and networks]*. Moskva: ID «FORUM»: INFRA - M, 2017, 416 p. (in Russian).
6. A.I.Baranchikov, P.A.Baranchikov, A.N.Pyl'kin, *Algoritmy i modeli ogranicheniya dostupa k bazisu dannykh [Algorithm and model and database access restrictions]*. Moskva: Goryachaya liniya - Telekom, 2016, 182 p. (in Russian).
7. A.A.Vnukov, *Osnovy informatsionnoy bezopasnosti: zashchita informatsii [Fundamentals of information security: information protection]*. Moskva: Izdatel'stvo Yurayt, 2019, 240 p. (in Russian).
8. N.A.Olifer, *Komp'yuternyye seti. Printsipy, tekhnologii, protokoly [Computer networks. Seals, technologies, protocols]*. Sankt-Peterburg: Piter, 2002, 672 p. (in Russian).
9. Ye.V.Vostretsova, *Osnovy informatsionnoy bezopasnosti [Fundamentals of information security]*. Yekaterinburg: Izd - vo Ural. un - ta, 2019, 204 p. (in Russian).
10. S.A.Nesterov, *Osnovy informatsionnoy bezopasnosti [Fundamentals of information security]*. Sankt-Peterburg: Lan', 2017, 324 p. (in Russian).
11. A.YU.Shcheglov, *Zashchita komp'yuternoy informatsii ot nesanktsionirovannogo dostupa [Protection of computer information from unauthorized access]*. Nauka i tekhnika, Sankt – Peterburg, 2004, 384 p. (in Russian).
12. V.A.Galatenko, *Osnovy informatsionnoy bezopasnosti [Fundamentals of information security]*. Moskva: Izdatel'stvo ―INTUIR.RU, 2003, 280 p. (in Russian).
13. Blyth Andrew, Kovacich Gerald, *Information Assurance: Security in the Information Environment (Computer Communications and Networks)*. Springer, 2006, 264 p.
14. A.V.Vasil'kov, I.A.Vasil'kov, *Bezopasnost' i upravleniye dostupom v informatsionnyye sistemy [Security and access control to information systems]*. Moskva: FORUM: INFRA - M, 2013, 368 p. (in Russian).
15. Menga Justin, Timm Carl, *CCSP: Secure Intrusion Detection and SAFE Implementation Study Guide*, Sybex, 2004, 725 p.
16. R.Pauer, “Eksperty diskutiruyut o nastoyashchem i budushchem sistem obnaruzheniya atak” [Experts discuss the present and future of attack detection systems], *Computer Security Journal*, vol. XIV, pp. 5–12, 2001. (in Russian).
17. Riptech Internet Security Threat Report. Attack Trends for Ql and Q2 2002. Volume II. Riptech, Inc. July 2002.
18. G.P.Zhigulin, *Organizatsionnoye i pravovoye obespecheniye informatsionnoy bezopasnosti [Organizational and legal support of information security]*. Sankt-Peterburg: NIU ITMO, 2014, 173 p. (in Russian).
19. A.L.Denisova, Ye.V.Zaytsev, *Teoriya i praktika ekspertnoy otsenki tovarov i uslug [Theory and practice of expert evaluation of goods and services]*. Tambov: Izd-vo Tamb. gos. tekhn. un-ta, 2002, 72 p. (in Russian).