UDC 65.012 DOI: 10.20998/2413-3000.2018.1278.10

V. K. KOSHKIN, A. V. MANDRA

SECURITY SYSTEM INTEGRATION IN INFORMATION SYSTEMS FOR IT PROJECTS

The frequency of unauthorized actions to information systems (IS) in the process of their integration is steadily increasing, which inevitably leads to huge financial and material losses. According to statistics, internal users of IS, commit more than half of all violations. All of this forms "a dangerous group of risk". Existing approaches for IS security are mainly provided by specialized tools of differentiation of user access to information resources. The legal maintenance of information security is a set of laws, legal documents, regulations, instructions, manuals, requirements which are required in the information security system. Organizational and administrative support of the information security is a regulation of industrial activity and the relationship between performers in the legal and regulatory basis in the way that disclosure, leakage and unauthorized access to information come impossible or significantly hampered by carrying out organizational activities. The technical tools of protection include the hardware, software and cryptographic protection, which make difficult to attack, and help detect the fact of its occurrence, and help to get rid of the consequences of an attack. Behavioral methods, unlike signature, is based on models of IS with regular process operation and not based on information attacks models. The principle of behavioral methods is to detect discrepancies between the current modes of the operation of IS and full-mode model is laid down in the method parameters. Any such discrepancy is considered as an information attack. The algorithm of the signature method concerns to find the source of attack signatures in the data collected by the network and host intrusion detection system sensors. In the case that the required signatures are founded, intrusion detection system records the fact of the information attack, which corresponds to the signature found. The disadvantage of this group of methods is the difficulty of creating accurate models of the normal mode of IS functionality.

Keywords: Information system, intrusion detection system, behavioral method, signature method, security of information systems.

В. К. КОШКІН, А. В. МАНДРА

ІНТЕГРАЦІЯ СИСТЕМИ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЛЯ ІТ-ПРОЕКТІВ

Частота несанкціонованих дій інформаційних систем (ІС) у процесі їх інтеграції неухильно зростає, що неминуче призводить до величезних фінансових та матеріальних збитків. За статистикою, внутрішні користувачі ІС, здійснюють більше половини всіх порушень. Все це формує "небезпечну групу ризику". Існуючі підходи до безпеки ІС в основному забезпечуються спеціалізованими інструментами диференціації доступу користувачів до інформаційних ресурсів.

Ключові слова: інформаційна система, система виявлення вторгнень, поведінковий метод, метод підпису, безпека інформаційних систем.

В. К. КОШКИН, А. В. МАНДРА

ИНТЕГРАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ДЛЯ ИТ-ПРОЕКТОВ

Частота несанкционированных действий в информационных системах (ИС) в процессе их интеграции неуклонно возрастает, что неизбежно ведет к огромным финансовым и материальным потерям. Согласно статистике, внутренние пользователи ИС совершают более половины всех нарушений. Все это образует «опасную группу риска». Существующие подходы к обеспечению безопасности ИС в основном предоставляются специализированными инструментами дифференциации доступа пользователей к информационным ресурсам.

Ключевые слова: информационная система, система обнаружения вторжений, метод поведения, метод подписи, безопасность информационных систем.

Introduction. In recent years, the frequency of unauthorized actions into information systems (IS) is constantly increasing, which inevitably leads to huge financial and material losses. There is an interesting fact, more than half of all violations committed by the company's employees, i.e. internal IS users. It is known that for the last few years, IS protection from insiders is mainly provided by specialized tools of the differentiation of user access to information resources. With the help of these tools to each user are assigned specific rights, in accordance with this it is permitted (or prohibited) local access to information are stored in a computer, or remote access via communication links to information on other computers [1]. It must be noted that this approach does not solve the whole problem of information sources protection from intruders are operating inside IS. This is caused by two main factors:

- tools of differentiation of local access are not able to provide protection against the actions of offenders who are not directly related to obtaining unauthorized access to information system resources. For example, the user can intentionally install and run the malicious software on own workstation that allows to capture and analyze network traffic in the IS. Another example of the unauthorized activity when protection can't be ensured by tools of access control is data recorded to external devices or the printing of confidential information to which the user has legally access. To identify such actions in IS should apply the system of workstation active monitoring;

- the tools of differentiation of remote access does not provide protection from network attacks that can be performed by internal users of the system. Such attacks are based on vulnerabilities that may happen in software-hardware server and desktop stations of IS. Examples of vulnerabilities are unstable passwords, incorrect software configuration, errors are presented in the application software, etc. The success of the network attacks can lead to a breach of confidentiality, integrity or availability of information in the system. To timely detect and block such attacks should be used detection tools, known as

IDS-system (Intrusion Detection Systems) [2].

The main tasks of research:

- the development of organizational measures needed to meet the requirements of data protection, organizational and administrative documentation projects;
- the ensure compatibility of hardware and software processing tools of data protection on the protected workstation with installable protection tools in compliance with the requirements for the configuration mechanisms of closed software environment, and flow control (mandatory access);
- the organization of complex schemes of information backup to external devices;
- the development of the efficient schemes of the operational and centralized management of configuration;
- the development of regulations to ensure continuity and rapid recovery of the functioning of the object of protection in the presence of complex server groups, including the secure server and domain controller, database, a management server anti-virus tools and file server.

Thus, the effective protection from insiders of information security requires the use of additional forms of protection, such as workstations active monitoring, as well as intrusion detection systems.

The main methods of ensuring the security of information systems

The main methods of ensuring the security of information systems.

In order to counter threats are listed in the previous, modern information systems include security engines that implement the adopted security policy. Security policy in accordance with the purpose and conditions of operation of the system can determine the rights of access to resources and regulate the procedure of auditing of user activity in the system of network communications protection, to formulate ways of restoring the system after random crashes, etc. For the implementation of the adopted security policy, there are legal, organizational, administrative and engineering measures to protect information (see fig. 1). The legal maintenance of information security is a set of laws, legal documents, regulations, instructions, manuals, requirements which are required in the information security system.

Engineering measures are a set of special authorities technical tools and measures which are operating together to perform a specific task on the Data Protection Act. To engineering tools is included screening rooms, the organization of alarm, security facilities with a PC.

Organizational and administrative support of the information security is a regulation of industrial activity and the relationship between performers in the legal and regulatory basis in the way that disclosure, leakage and unauthorized access to information become impossible or significantly hampered by carrying out organizational activities [3,4].

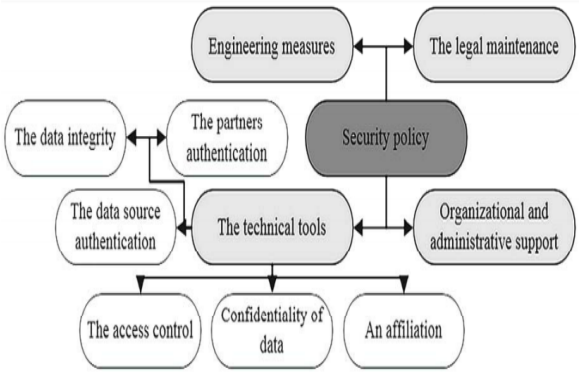

Fig. 1 – The structure of security policy

Measures of this class include the selection and training of personnel, the definition of job descriptions of employees, an organization of access control, security of premises, the organization of information security with the conduct of control of personal information, determining the order of storage, redundancy, destruction of confidential information, etc. The technical tools of protection include the hardware, software and cryptographic protection, which make difficult to attack, and help detect the fact of its occurrence, and help to get rid of the consequences of an attack.

Technical tools of security subsystems in modern distributed information systems have the following main features:

- the partner's authentication on the interaction, which allows ensuring in the authenticity of the partner when the connection is established;
- the data source authentication, which ensures in authenticity of the source of the message;
- the access control to protect against unauthorized use of resources;
- confidentiality of data, which provides protection against unauthorized information;
- the data integrity for detection and, in some cases, and prevent change of information when its storage and transfer;
- an affiliation, which provides proof of the belonging information to a certain person. The intrusion detection system.

The intrusion detection system. Detection systems are designed to detect attacks and counter network attacks from intruders. Intrusion Detection Systems (ISD) are specialized software and hardware with a standard architecture [5], which includes the following components (see fig. 2):

- Sensors-modules to collect the necessary information about the network traffic in IS;
- The Module of attacks detection that performs data processing are collected by sensors to detect phishing attacks;
- The Response Module for detected attacks;
- The Storage Module of Configuration Information, as well as information about detected attacks;

- That unit usually performs a standard database (e.g. MS SQL Server, Oracle or DB2);

- The Control Module of Components of intrusion detection system.

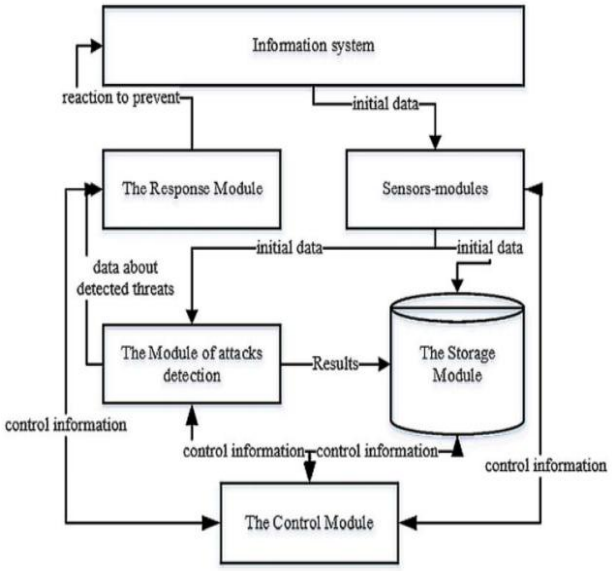

Fig. 2 – The typical architecture of intrusion detection systems

The two types of sensors are needed to be used in the intrusion detection system - the network and host. Networked sensors are designed to collect information about the data packets are transmitted in the IS segment, where the sensor is installed. Host sensors are installed on the IS servers and are designed to collect information about the data packets that are received by the server with the sensor.

The information is collected by the network and host sensors further will be analyzed by the intrusion detection system to identify the potential violators of attacks. The data analysis can be carried out by two main groups of methods - signature-based and behavioral [6].

Signature methods describe every attack in the form of a special model, or signature. As the signature attacks can be: character string, semantic expression in a special language, a formal mathematical model, etc. The algorithm of the signature method concerns to find the source of attack signatures in the data collected by the network and host intrusion detection system sensors. In the case that the required signatures are founded, intrusion detection system records the fact of the information attack, which corresponds to the signature found. The advantage of the signature methods is their high precision and obvious disadvantage - the inability to detect the attacks that are not identified by the methods of signature.

Behavioral methods, unlike signature, is based on models of IS with regular process operation and not based on information attacks models. The principle of behavioral methods is to detect discrepancies between the current modes of the operation of IS and full-mode model is laid down in the method parameters. Any such discrepancy is considered as an information attack. The advantage of this type of methods is the ability to detect new attacks without the need for constant change operating parameters of the module. The disadvantage of this group of methods is the difficulty of creating accurate models of the normal mode of IS functionality.

After identifying the attack in the IS the intrusion detection system has the ability to take specific response action to block it. For the implementation of these actions is responsible the response module of intrusion detection system. The responding in intrusion detection system can be inactive and passive form. To passive methods of response refers simply notify the administrator of the intrusion detection system about detected attacks. To the active can be included the following methods:

- The block of TCP-connection, in which the attack was realized. Such a closure is realized by sending special subjects TCP-connection segment with the RST flag set;

- The launch of an external program with a given certain parameters. The presence of such response functions of the module allows to administrator of intrusion detection systems complements existing methods of responding with their own methods, are implemented in the form of external software;

- The reconfiguration of the firewall with the purpose of blocking traffic is coming from the offending host. Currently, the vast majority of the existing DOE has the appropriate external interfaces, which provide the interaction with the firewall of intrusion detection system. An example of such an interface is an OPSEC interface for firewall CheckPoint FW-1.

According to the fact that the intrusion detection systems can themselves act as a malicious attack objects, these systems must be equipped with its own security subsystem.

However, it should be noted that a single use of intrusion detection systems doesn't allow completely solve the problem of protection against unauthorized activities of internal users of IS. This is primarily connected with the fact that the intrusion detection systems detect only the information attacks that can be detected by analyzing only the data packets circulating in the IS. This fact does not allow intrusion detection systems to detect unauthorized actions of those users who are not connected to a network of IS traffic.

The systems of active monitoring of IS workstations, as well as intrusion detection systems, are designed to detect and block phishing attacks, but not at the network level but at the level of the IS workstations.

The architecture of active monitoring systems is similar to the structure of the intrusion detection system. The sensors of the active monitoring system are installed into the workstations of IS users and allow to collect information about all events are taking place. An example of such information may be:

- about the applications are running at workstations;

- about the users are working at the station at the current time;

- on file access to applications;

- about the network traffic that is generated by IS applications, and others.

The collected information is fed into the analysis module of active monitoring system where data processing is carried out. The security administrator must

pre-configure of analysis module of the active monitoring system, i.e. define requirements that allow or deny IS users perform various operations at the workstations. The totality of these requirements is a security policy in the active monitoring system, which can be a part of a whole organizational security policy. For example, according to some defined security policy work with printers or access to certain files can be prohibited to some users.

Conclusion. The current strategy of information systems protection is should be partially reviewed. According to the fact that for a long time, this problem was solved only with the tolls of access control, so completely protect the IS from insiders it was not possible. It connects to the fact that the functionality of these tools does not allow to protect the IS from the internal network attacks, as well as the actions of internal users of IS, which is not directly related to the violation of the access rules restricting to the information resources of IS.

To protect information security from internal threats it needs to use ISD and active monitoring system. The sensors of ISD are installed at servers of the intrusion detection system and IS workstation and perform the functions of detection the network attacks by analyzing network traffic. The sensors of the active monitoring system are installed on users workstations of IS and allow to detect and block the actions of users who violate the specified policy. The sharing use of intrusion detection systems and active monitoring systems allow to use a comprehensive approach in the protection against internal attacks and significantly improve the level of information security in IS.

References

1. *Information System Security Associated*. 2013. Available at: http://www.issa.org
2. Chang SE, Ho CB. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*. 2006, no. 106 (3), pp. 345-361.
3. Chari SN, Cheng PC. BlueBox: A policy-driven, host-based intrusion detection system. *ACM Transactions on Information and System Security (TISSEC)*. 2003, no. 6 (2), pp. 173-200.
4. Chebrolu S., Abraham A., Thoma J. P. Feature deduction and ensemble design of intrusion detection systems. *Computers & Security*. 2005, no. 24 (4),. pp. 295-307.
5. Hinde S. Privacy legislation: A comparison of the US and European approaches. *Computers & Security*. 2003, no. 22 (5), pp. 378.
6. Kenkre P. S., Pai A., Colaco L. Real-time intrusion detection, and prevention system. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer International Publishing, 2015, pp. 405-411.

Received 15.12.2017

Відомості про авторів / Сведения об авторах / About the Authors

Кошкін Володимир Костянтинович **(*Кошкин Володимир Костянтинович, Koshkin Volodymyr Konstantinovich*)** – кандидат технічних наук, викладач кафедри програмного забезпечення автоматизованих систем Національного університету кораблебудування імені адмірала Макарова, г. Николаев, тел .: +38 (063) 7493942, e -mail: koshkin-vladimir@mail.ru. ORCID: 0000-0002-7318-1856.

Мандра Андрій Валерійович **(*Мандра Андрей Валерьевич, Mandra Andriy Valerievich*)** – Національний університет кораблебудування імені адмірала Макарова, викладач кафедри інформаційних управляючих систем та технологій, м. Миколаїв, тел.: +38 (066) 0772799, e-mail: mandra.andrew@gmail.com. ORCID: 0000-0002-0917-5857.