Conference Paper

The Methodology of Detection of Internal Infringers in the Information System

K. A. Zhukov

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse, 31, Moscow, 115409, Russia

Abstract

This article provides the classification of infringers of safety of information system (IS), the methodology of construction of model of the internal infringer of safety of information system is represented, existing methods and phases of detection of internal infringers of information system are considered.

Keywords: internal infringers, information system, infringers of safety, threats to the IS, model of the internal infringer

Corresponding Author:
K. A. Zhukov

Received: 22 July 2018
Accepted: 9 September 2018
Published: 8 October 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the Breakthrough Directions of Scientific Research at MEPhI Conference Committee.

1. Introduction

The Development of modern information and communication technologies influences many spheres of human activity, raising their efficiency in the process and, simultaneously, generating a set of uncontrollable threats, including those in the information sphere. Bearing this in mind the requirements for the protection of crucial information resources are constantly on the raise. For today, key and defining international regulatory legal acts in the field of management of information security and information protection is a series of standards ISO 27k [1].

The management of incidents, according to the international standard ISO/IEC 27035: 2011, allows to reveal, analyze and effectively investigate the incidents of information security in due time, for minimization of negative consequences for information systems and the organizations.

The essential contribution to the development of detection of internal infringers to information system was brought by such domestic and foreign scientists as: A. P. Mihalkova, A. S. Zaycev [2], S. V. Volobuev [3], A. L. Golubenko, V. A. Horoshko, A. S. Petrov, E. V. Belozerov [4], A. I. Zaharov [5], I. A. Kovtun, V. I. Muhan, J. I. Naboka [6], J. Biskup [7], etc.

2. Classification of Infringers of Safety of Information System

The analysis of existing means and methods of protection of information system states that in overwhelming majority the methods for providing information security of the IS offer protection of the data exclusively from external infringers (malefactors), there forgetting about the internal ones.

The solid ground for such position is the assumption on the professional competence of the users of the information system. However, it is not entirely true. Nowadays there is a necessity for the development of the possible types of infringers. In relation to IS, infringers can be internal (from among the employees, users of system) or external (unauthorized users or any persons who are outside of a controllable zone) (Table 1).

Table 1: Classification of infringers of safety of information system.

External	Internal
Random visitors	Officials, chiefs of services of the information security
Hackers	Development and support team personnel (Applied and system programmers)
Criminal organizations	Users of the system
Developers	Heads of different levels of official hierarchy
Partners	Technical personnel

In each specific case, proceeding from the technology of data processing, a model of an internal or external malefactor, adequate to the real malefactor for given IS, is developed. It is necessary to mind that the model of the internal infringer – the abstract formalized or non – is a formalized description of actions of the malefactor, which reflects its practical and theoretical possibilities, one's aprioristic skills, time and a scene of action and etc.

For the construction of the given model, it is recommended to analyze and sort out the following information.

The internal malefactor should be considered as the person who aspires to gain unauthorized access to the information circulating in an information system. For the construction of a model of the internal infringer, it is necessary to consider that the first feature of IS resources is the accessory to certain people or certain groups of persons who for the purpose of the use of these resources aspire to be users of the information circulating in the IS. This accessory is often created by the character and the volume of the information that is entered, processed, stored and circulated in IS,

more often. If a certain person is the internal user of resources of the IS and carries out an attempt of unauthorized access to the objects of security such user is considered to be an internal infringer.

The model of the internal infringer should define:

1. categories of people from which there can be an infringer;
2. level of skill of the internal infringer;
3. the assumption of qualification and a possible level of the infringer's knowledge;
4. methods and the ways used during the violations;
5. the possible target of the infringer and its degree of danger for the IS;
6. possible places of violations;
7. possible ways for the realization of violations in IS; and
8. the assumption of character of the infringer's actions.

For the categories of people that can be infringers, it is necessary to relate:

1. the subjects of information activity of the IS: employees of the organization, owner of the IS, internal infringers; for their detection it is necessary to examine in detail the possibilities of unauthorized access to resources of the IS among the employees of the organization;
2. external persons who get in one way or another access to the resources of the IS: external malefactors; for whose definition it is necessary to consider in detail their possibilities of visiting the organization to gain unauthorized access to the resources of the IS, considering the existing system of organizational restrictions to the access.

3. Methodology of Detection of Internal Infringers of the Information System

The methodology of detection of internal infringers of the IS includes two phases: passive and active. During a passive-phase search and identification of attacks, with the application of such methods as:

1. the analysis of signatures of activity;

2. statistical methods of the analysis (the behavior analysis); and
3. dynamic (smart) analysis.

The method of the analysis of signatures means the presence of protection of the knowledge base of signatures in information systems that are strictly certain descriptions of existing kinds of activity of the internal infringer. The given method of detection of infringers is one of the most popular because of its partial simplicity of action and effective speed of search. An essential minus of the given method is an absence of detection of the infringer whose signatures are not present in a database.

Statistical methods of the analysis are intended for the purpose of search of activity of the internal infringer that differs from the usual activity for the given information system. The given methods of the analysis provide the possibility to define internal infringers, before that unknown to the security system. However, it is important to notice that the given methods often enough possess higher probability of essential errors, and also do not give a possibility to conduct a search for the internal infringers in real time.

The dynamic analysis – is the search of activity of the infringer similar to the attacks that are known to the information system. The given method of the analysis is an intellectual one as there are algorithms of generalization and classification of the data contained in it, and it gives possibility to generate new knowledge from already existing one. Because of difficulties of initial adjustment and low speed of training of system of the security, this method of the analysis is almost unused. As a rule, methods of the dynamic analysis are combined with signature ones, and the base of signatures acts as a storehouse of knowledge. This method of the analysis is called hybrid or combined.

After detection and identification of the infringer, the security system of the IS carries out its registration by:

1. data recording of the attack to the system's registry of events;
2. generating a message on the console of the security manager; and
3. mailing of messages by e-mail, through the services of instant messages.

The active phase of counteraction to the internal infringer is carried out by means of following methods:

1. Cancellation of session of the infringer who is making an unauthorized action;
2. Blocking of the account of the internal infringer;

3. Misinformation of the internal malefactor;
4. Change of the configuration of gateway screens and routers;
5. Suppression of the local displays of attack on the IS;
6. Reshuffle of anti-virus programs of the IS; and
7. Reciprocal attacks on the system of the internal infringer.

4. Conclusion

As a conclusion, the results of the research will be shown. According to the results of the research of Agency CNews Analytics (CNA), the most serious threats of security of IS are the systematic information leakage (70%) and negligence of the internal personnel (70%). Limitations of modern security systems of the IS are connected with the fact that internal infringements are much more difficult to highlight and diagnose than the external ones. Actions of own employees can be unpredictable or strengthened possibilities of unapproved access or theft of the data. The amount of harm can be considerable higher than from the influence of external infringers.

As to prevention measures, it is considered that rigid restriction of access for the personnel is not effective and can lead to malfunction of all IS. Internal security is always the compromise between organizational and technical methods, aspiration to security and requirements of the IS. At the same time, it is an ongoing process that provides not only introduction and adjustment of program decisions, but also constant work and personnel training.

References

[1] Higgins, S. (2009). *Information Security Management: The ISO 27000 (ISO 27K) Series*, T. 19. Digital Curation Centre (DCC).

[2] Mihalkova, A. P. and Zaycev, A. S. (2015). On the application of the Bayesian approach for early detection of internal infringers of information security. *Information Technology Security*, T. 22, no. 3.

[3] Volobuev, S. V. (2000). On the systematization of the detection and analysis of leakage channels. *Direct and Indirect Media/Information Security Issues*, no. 1, pp. 26–37.

[4] Golubenko, A. L., Horoshko, V. A., Petrov, A. S., et al. (2006). Information technology and cybercrime. *Bulletin of SNU*, vol. 103, no. 9, pp. 7–10.

[5] Zaharov, A. I. (2005). Information systems: Risk assessment. *Information Security*, no. 6, pp. 18–19.

[6] Kovtun, I. A., Muhan, V. I., and Naboka, J. I. (2001). Types of information impacts. *Information Security Issues*, vol. 52, no.1, pp. 2–7.

[7] Biskup, J. (2009). *Security in Computing Systems: Challenges, Approaches and Solutions: Monograph*, p. 694. Berlin: Springer.