INTERNATIONAL JOURNAL • ENGINEERING RESEARCH •

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 20 th June 2021.
Link: https://ijiemr.org/downloads/Volume-10/ISSUE-6

DOI: 10.48047/IJIEMR/V10/I06/22

Title: **MODEL OF THE INFORMATION SECURITY PROFILE OF THE CORPORATE INFORMATION SYSTEM**

Volume 10, Issue 06, Pages:112-116

Paper Authors: **O’rinov Nodirbek Toxirjonovich, Abduraxmanov Jamolidin Komoldinovich**

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

MODEL OF THE INFORMATION SECURITY PROFILE OF THE CORPORATE INFORMATION SYSTEM

O'rinov Nodirbek Toxirjonovich,
Teacher, Department of Information Technology, Andijan State University
E-mail: nodirbekurinov1@gmail.com

Abduraxmanov Jamolidin Komoldinovich
Candidate of physical and mathematical sciences, Department of Information Technology, Andijan State University
E-mail: jamolidinkamol@gmail.com

Abstract: The aspects of managing threats to information security of corporate information systems are considered. Vulnerabilities typical for corporate information systems are highlighted. The sources of threats have been identified. Potential violators are described. A unique model of the information security threat profile of a corporate information system has been developed.

Keywords: threat profile, threat classification problem, list of threats, threat sources, vulnerabilities, corporate information system, management, information security.

Introduction

Information security (IS) in corporate information systems (CIS) is gaining popularity in modern society of scientific and technological progress [8]. The relevance of building secure corporate information systems is increasing due to the growth of small and large enterprises, as well as an increase in the need for procedures for combining organizations and enterprises into a corporation [8; fourteen]. The construction of secure corporate information systems is based on assessing the level of information security in the event of the implementation of threats to their information resources [1; four; eight]. The authors of [1] noted that in the implementation of IS threats, enterprises incur material, reputational and financial losses. Thus, the basic operation in ensuring IS of a corporate information system is the development of a threat model inherent in this corporate information system.

Related work and proposed solutions

The work [2; 3; 6-11; 13]. The authors of the publication [2] describe the types of information threats, on the basis of which the classification of attacks has been developed. However, work [2] focuses on SCADA systems and network security. The authors in the study [6] propose a risk reduction strategy based on threat management. In particular, [6] describes the following threat management procedures: evading a threat or eliminating a threat source, reducing the level of vulnerabilities through the use of protective measures, reducing the negative consequences of the implementation of threats [6]. For the first time, the concept of a threat profile was investigated by the author of [3]. In [3] it is noted that the threat profile is associated with the life cycle of the IS and allows you to describe IS threats both qualitatively and formalized. Analysis [7; nine; 13] shows that the basic procedure for the classification of information resources (IR) is a prerequisite for the need to determine the list of threats. Thus, for each IR or IR group, it is necessary to determine a list of threats in the ratio of confidentiality, integrity and availability in order to identify vulnerabilities for each identified threat. The reason for this is the possibility of implementing a threat using vulnerabilities [2; eleven; 13]. According to the study [9], the threat profile is described by static attributes (identity of the threat, method of implementation, object of protection, source of threats, vulnerability).

The problem of classifying IS threats to a corporate business system is especially important for systems operating at industrial enterprises and in design bureaus [2; 13].

Thus, most of the studies carried out are devoted to the problem of managing information security threats and their analysis in industrial and information systems. However, this problem has not been practically solved in the CIS. Consequently, there are prerequisites for the need to develop a threat profile, the use of which will allow implementing a risk-oriented approach [11]. Using the list of IS threats, it is possible to build an enterprise IS management system, which will allow the enterprise infrastructure to have the property of protecting information used in the business processes of the enterprise [13].

The proposed model

The authors of the article propose a model of a corporate information security threat profile (see figure), based on the object of threats and the purpose of their implementation. This property of the threat is described by the authors of [8]. The purpose of the implementation of threats (both a single threat and a set of threats) is to disable the protective mechanisms of the corporate information system [8] and activate the vulnerabilities of the corporate information system [6; 12]. Based on this, it is possible to single out the main goal of the functioning of the information security system (ISS) of the CIS: countering threats to the security of the CIS.

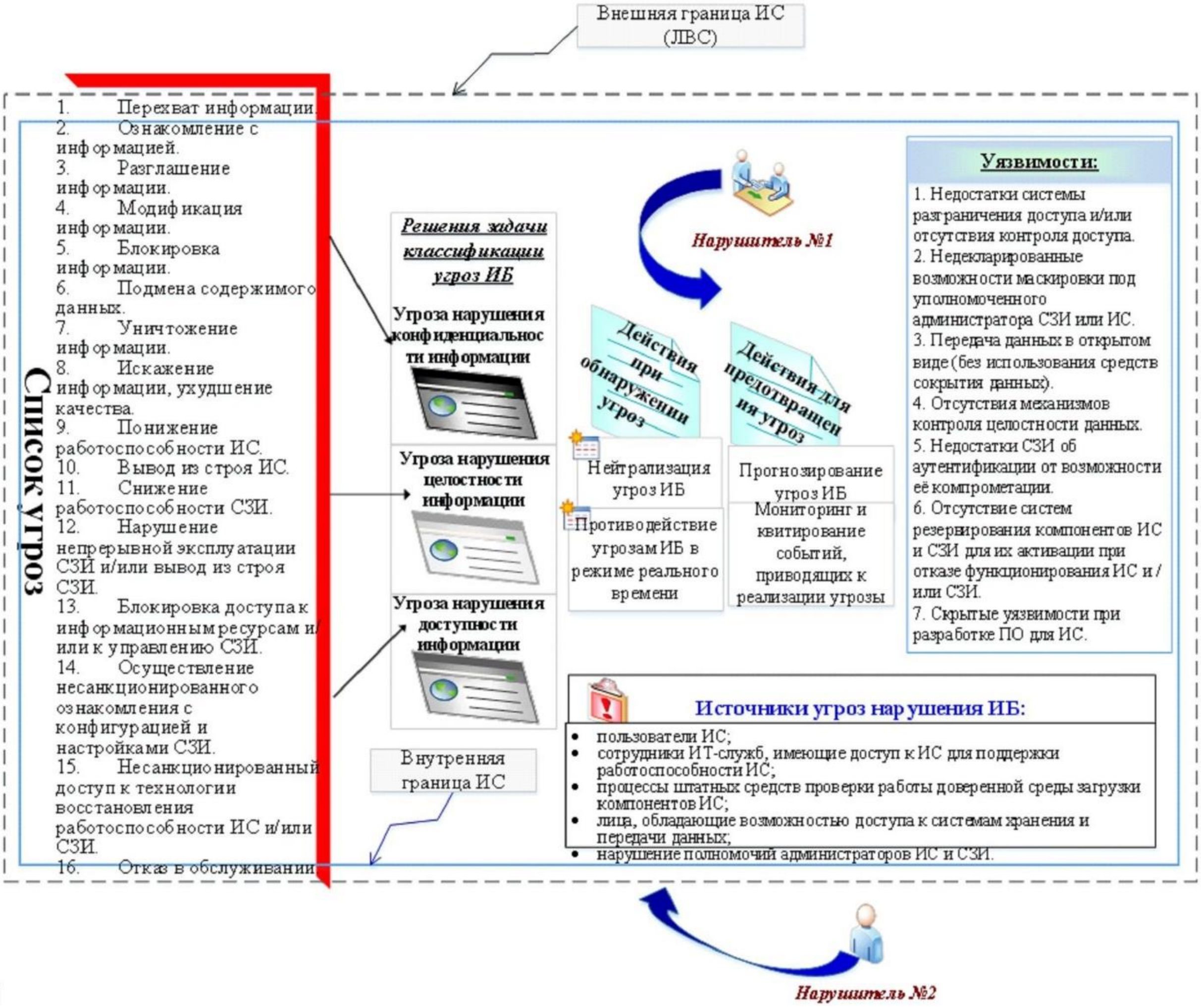
The model (see figure) describes the current threats specific to the corporate information system using the components: "list of threats", "sources of threats", "vulnerabilities". These threats are comparable to seven vulnerabilities, starting from which, an attacker can attack the corporate information system, its components and the computer network (BC) in which it operates. A threat profile has a step-by-step description of how to detect and prevent threats if necessary. The model defines the types of offenders: offender No. 1 - “internal”, offender No. 2 - “external”. An internal intruder is a person who is a user or administrator of this CIS. An external offender can be employees of the enterprise who are not users of the corporate information system, or other persons who are not part of the working personnel of the enterprise. The scope of the attackers is shown by an arrow (see figure). Attacking actions of an external attacker are aimed at the external border of the corporate information system, mainly at the aircraft, information and communication technologies, information security systems located at the border of the aircraft to form a secure connection between the aircraft and the corporate information system. Attacking actions of an internal attacker are carried out inside the CIS: on IS components, software, application applications, databases, information resources, means of access control.

The focus of IS threats is formed by the threat source. Several such sources are characteristic of corporate information systems, five of them were identified during the development of protection profiles:

1) users of a corporate type information system or information systems, united into a single management link;
2) employees of departments of IT services who have access to the CIS to support its performance;
3) functional processes of built-in (standard) tools for checking the operation of a trusted loading environment for IS components;
4) persons who have the ability to access data storage and transmission systems;
5) violation of powers by the administrators of IS and ISS.

Information security threat profile model of a corporate information system

Application of the IS threat profile allows solving the problem of classifying IS threats by dividing them into three types: violation of the integrity, availability and confidentiality of information, which is interconnected with the classification of security threats given in [6], and allows you to implement the recommendations of the method [14].


Внешняя граница ИС (ЛВС)
Список угроз
1. Перехват информации.
2. Ознакомление с информацией.
3. Разглашение информации.
4. Модификация информации.
5. Блокировка информации.
6. Подмена содержимого данных.
7. Уничтожение информации.
8. Искажение информации, ухудшение качества.
9. Понижение работоспособности ИС.
10. Вывод из строя ИС.
11. Снижение работоспособности СЗИ.
12. Нарушение непрерывной эксплуатации СЗИ и/или вывод из строя СЗИ.
13. Блокировка доступа к информационным ресурсам и/или к управлению СЗИ.
14. Осуществление несанкционированного ознакомления с конфигурацией и настройками СЗИ.
15. Несанкционированный доступ к технологии восстановления работоспособности ИС и/или СЗИ.
16. Отказ в обслуживании.
Решения задачи классификации угроз ИБ
Угроза нарушения конфиденциальности информации
Угроза нарушения целостности информации
Угроза нарушения доступности информации
Внутренняя граница ИС
Нарушитель №1
Действия при обнаружении угроз
Действия для предотвращения угроз
Нейтрализация угроз ИБ
Противодействие угрозам ИБ в режиме реального времени
Прогнозирование угроз ИБ
Мониторинг и квитирование событий, приводящих к реализации угрозы
Уязвимости:
1. Недостатки системы разграничения доступа и/или отсутствия контроля доступа.
2. Недекларированные возможности маскировки под уполномоченного администратора СЗИ или ИС.
3. Передача данных в открытом виде (без использования средств сокрытия данных).
4. Отсутствия механизмов контроля целостности данных.
5. Недостатки СЗИ об аутентификации от возможности её компрометации.
6. Отсутствие систем резервирования компонентов ИС и СЗИ для их активации при отказе функционирования ИС и / или СЗИ.
7. Скрытые уязвимости при разработке ПО для ИС.
Источники угроз нарушения ИБ:
• пользователи ИС;
• сотрудники ИТ-служб, имеющие доступ к ИС для поддержки работоспособности ИС;
• процессы штатных средств проверки работы доверенной среды загрузки компонентов ИС;
• лица, обладающие возможностью доступа к системам хранения и передачи данных;
• нарушение полномочий администраторов ИС и СЗИ.
Нарушитель №2

Conclusion

The security of the information assets of the enterprise in which the corporate information system is implemented depends on the level of IS maintenance of the corporate information system. To protect the data processed in the corporate information system, it is advisable to provide the IS of the system itself, to identify and predict the threats of IS violation. Such measures will ensure effective information security management and a high-quality response to corporate information security threats in real time. Thus, the research carried out on the problems of threat management and ensuring IS KIS allowed the authors of the article to develop a model of the profile of IS IS KIS threats. The difference from the previously proposed models is that the proposed solution defines the actions to be taken when threats are detected and to prevent them. The application of the proposed model in practice will make it possible to implement special procedures for managing an enterprise 's information security threats, using private information security policies for corporate information systems.

BIBLIOGRAPHY

1. Azhmukhamedov, I. M. Assessment of the state of security of an organization's data in the context of the possibility of implementing threats to information security / I. M. Azhmukhamedov , O. M. Knyazeva // Caspian journal: management and high technologies. - 2015. - No. 3 (31). - S. 24–39.
2. Analysis of information risks in data processing systems based on "foggy" calculations / A. A. Finogeev, A. G. Finogeev, I. S. Nefedova, E. A. Finogeev, V. A. Kamaev // Bulletin of the Astrakhan State Technical University ... Series: Management, Computer Engineering and Informatics. - 2015. –No. 4. - P. 38–46.
3. Astakhov, A. M. Art of information risk management / A. M. Astakhov. - M.: DMK Press, 2010 .-- 314 p.
4. Babenko , A . A . Information security model in the segment of corporate information system / A . A . Babenko , On . With . Kozunova // Information systems and technologies . - 2017. - No. 1 (99). - With . 87-91.
5. The basic model of threats to the security of personal data during their processing in personal data information systems: (extract): approved. Deputy Director of FSTEC of Russia 15 Feb 2008 - Electron. text data. - Access mode: https://fstec.ru/component/attachments/download/289 (date of access: 06.02.2018). - Zagli . from the screen.
6. Vybornova , ON , Azhmukhamedov IM Synthesis of management decisions to reduce risks in fuzzy conditions with limited resources / ON Vybornova , IM Azhmukhamedov // Fundamental research. - 2016. - No. 5 (part 1). - S. 18–22.
7. Kozunova , S. S. Management of threats to information security of information systems / S. S. Kozunova // Concepts of fundamental and applied scientific research: collection of articles. Art. based on materials of Mezhdunar . nauch.- Pract . conf . (Ufa, December 9, 2017). At 6 o'clock, part 3 / hole ed .: A.A. Sukiasyan . - Sterlitamak, 2017. - pp. 69–71.
8. Kozunova , S. S. Model of building a secure information system of corporate type / S. S. Kozunova , A. A. Babenko // Information systems and technologies. - 2016. - No. 3 (95). - S. 112-120.
9. Kozunova , S. S. Risk resistance management of the information system of the design bureau / S. S. Kozunova , A. G. Kravets // Information security management in modern society: materials of the All - Russian . youth scientific. schools- conf . on information security (Volgograd, April 26–28, 2017) / editorial board : E. A. Maksimova, Yu. S. Bakhracheva , V. V. Baranov. - Volgograd, 2017. - pp. 203–207.
10. Methodology for determining actual threats to the security of personal data during their processing in personal data information systems: approved. Deputy Director of FSTEC of Russia 14 Feb 2008 - Electron. text data. - Access mode: https://fstec.ru/component/ attachments / download / 290 (date of access: 06.02.2018). - Zagli . from the screen.
11. Methods and models for assessing the infrastructure of the information security system in corporate networks of industrial enterprises: monograph / P. P. Paramonov, A. G. Korobeinikov, I. B. Tronikov , I. O. Zharinov. - SPb . : Studio "NP- Print ", 2012. - 115 p.
12. Modeling of network attacks of malefactors in the corporate information system / V. A. Gneushev , A. G. Kravets, S. S. Kozunova , A. A. Babenko // Industrial ACS and controllers. - 2017. - No. 6. - P. 51-60.
13. Nguyen , T. T. Messaging system based on the MQTT protocol / T. T. Nguyen , A. G. Kravets, N. Z. Bui // Topical issues of information security of regions in the context of globalization of the information space: materials of the VI All-Russian . nauch.- Pract . conf . (Volgograd, April 27–28, 2017) / editorial board : E. A. Maksimova [and others]. - Volgograd, 2017. - pp. 133–138.

14. Shevtsov, V. Yu. Features of secure document flow at the enterprise / V. Yu. Shevtsov, A. A. Babenko, S. S. Kozunova // Topical issues of information security of regions in the context of globalization of information space : materials of the V All-Russian . nauch.- Pract . conf . (Volgograd, April 22-23, 2016). - Volgograd, 2016. - pp. 237–341.