UDC 004.8 **doi: 10.26906/SUNZ.2018.3.100**

G. Golovko, M. Koltunov, A. Samofal

Poltava national technical Yuri Kondratyuk university, Poltava, Ukraine

PROBLEMS OF COMPREHENSIVE PROTECTION OF INFORMATION AT PJSC "RESEARCH AND DESIGN-PROCESSING INSTITUTE OF THE ENAMELED CHEMICAL EQUIPMENT AND NEW TECHNOLOGIES KOLAN"

The subject of research describes the peculiarities of the use of information security systems in the activities of PJSC "Research and Design-Processing Institute of the Enameled Chemical Equipment and New Technologies KOLAN". The essence of information security systems and the tasks that they can perform are defined. The **aim** is to take notice of comprehensive protection problems in enterprises. The following **results** are obtained. Information security performs four important for an organization which is protect the organization's ability to function, enable the safe operation of applications implemented on the organization's IT systems, protect the data the organization collect and uses, and lastly is safeguards the technology assets in use at the organization. **Conclusions.** The main components that form internal and external information security are defined. It is proved that the use of information security systems is an obligatory condition for the activity of a modern enterprise or production, which will help prevent the loss or theft of important sensitive information. Information security is crucial in organization. All information stored in the organization should be kept secure. Information security will be defined as the protection of data from any threats of virus. The information security in important in the organization because it can protect the confidential information, enables the organization function, also enables the safe operation of application implemented on the organization's Information Technology system, and information is an important asset for an organization

Keywords: protection, protection of information, information security, security of information.

Introduction

In the modern world, enterprise informational support and the introduction of new technologies are increasing. Now almost every enterprise, ranging from small firms to large corporations, has its own information systems. The main task of working with the information at the enterprise is the protection of its integrity, restriction of access to confidential information of third parties, the distinction of access to information of certain groups of employees, the establishment of a proper security system, as well as the encryption of confidential data of the enterprise. Implementation of information security systems at enterprises is a must for saving money, time and limiting access to confidential information. Recording of accounting documents, materials in stock, and raw materials, allows management to operate more effectively. At the enterprise there are systems that allow running the accounting information system and information systems for interaction with buyers. Lost or theft of information of such importance can cause losses or paralyze the workflow.

The purpose of researches. Analysis of the features of the use of modern comprehensive information security measures in the enterprise to prevent the loss or theft of strategic data at production. Study of the importance to introduce technologies and methods of their protection at the enterprise.

Analysis of recent research and publications. The analysis of scientific publications gives grounds to assert that in the process of designing, creating and operating information security systems there are errors and inaccuracies that significantly reduce the effectiveness of their operation. Development of information security policy that defines the strategy and tactics of the information security system in enterprise information systems and takes into account the dynamics of processes for changing the types and level of information threats, which is one of the active and significant resources of modern business environments, needs a separate justification for [1]. The system of information security in information systems of enterprises should be based on the principles of complexity and adaptability. It is advisable to develop an organizational structure and implement a system of information security in the information systems of enterprises in accordance with the recommendations of international standards and current legislation of Ukraine. Such standards are: ISO / IEC 27002 "Information Technology. Methods of protection. Code of Practice for Information Security Management"; ISO / IEC 27003 "Information Technologies. Methods of Protection: Guidelines for the Application of Information Security Management System"; ISO / IEC 27004 "Information Technology. Methods of protection. Measurement"; ISO / IEC 27005 "Information Technologies. Security Methods: Information Security Risk Management"; ISO / IEC 27006 "Information Technology. Security Methods. Requirements for the audit and certification of information security management systems"; ISO / IEC 27011 "Information Technology. Guidelines for Information Security Management for Telecommunications "[2]. Compliance with the ISO 27000 series standards ensures the management and control of the access, development and maintenance of hardware and software systems, and the management of the continuity of business processes. Compliance with ISO 27000 and compliance with national information security laws are essential for sustainable business development.

Presentation of the main result of research

Information security is the protection of information from the negative influences thereon. It relates to the technological protection procedures.

According to the requirements of the Laws of Ukraine "On Information", "On State Secrets" and "On the Protection of Information in Automated Systems", the main object of protection in information systems is information with restricted access, which is state or other, provided by the legislation of Ukraine, confidential information that is a state property or transferred to the state

in possession, use, disposal. In general, the object of protection in the information system is limited access information circulating and stored in the form of data, commands, messages that have a certain limitations and value for both its owner and potential intruder of technical protection of information. Intruder is a user who carries out unauthorized access to information [3]. By means of implementation, all information security measures are subdivided into legal (legislative), moral and ethical, organizational (administrative), physical and technical (software and hardware) ones. In our country there are changes at all levels of leadership and management, which are due to the intensive introduction of the latest information technology. The rapid improvement of information support, its penetration into all spheres of vital interests has, in addition to undeniable advantages, the appearance of a number of strategic problems. The risk of unauthorized interference into computer, information and telecommunication systems is increasing.

The urgency of the problem of protecting information and the safe use of information systems from various threats can be found out from the data published by Computer Security Institute in San Francisco, California, USA, according to which intrusions and interference into the work of information systems occurs for the following reasons: hacker attacks (unauthorized access) - 2%; viruses - 3%; hardware failure - 20%; targeted actions of workers - 20%; error in the work of employees - 55%. Thus, the human factor is the greatest threat, since the actions of workers make up 75% of intrusions and interference into the work of information systems.

The main task in reaching the information security protection of the information system is the limited access information that functions and is stored in the form of various data, commands, and messages. These data may be valuable not only to the owner but also to the potential intruder of technical protection of information.

Taking into account the economic situation of some companies, previous versions of the software are used to save money. Given that, for example, some versions of operating systems cease to be served after some time, they are successfully exploited by malicious people. Starting from May 12, 2017, a large number of computers with Windows operating system were under the virus attack by the WannaCry virus. The virus encrypted users' files so they could not be used; for decoding, the attackers demanded money. There were infected about 300,000 computers in at least 150 countries around the world. Losses were valued at more than $ 1 billion. A large number of state-owned companies in different countries suffered from the attack and more than 70% of the affected companies were in Russia and Ukraine. After the attack, Microsoft released security patches for operating systems that were no longer supported by the company, namely Windows XP, Windows Server 2003, and Windows 8 [4]. Therefore, experts advise using computers with important information without access to the Internet or protect them properly.

A high percentage of penetration of intruders occurs due to low-skilled workers who serve the information systems incorrectly. Most DDOS attacks occur due to the low qualification of system administrators who do not use network configuration in relation to incoming data packages. This is how the attacks are masked. In the absence of authorized user, control and delimitation of access to the terminal, the skilled intruder easily uses its functionality for unauthorized access to the information to be protected by entering appropriate requests or commands. In the presence of free access to the premises, one can visually observe information on means of storage and documentation, steal a paper carrier, make a copy, and steal other media with information: lists, magnetic media, etc.

A particular threat is the uncontrolled download of software that can change the settings, properties, data, algorithms, the introduction of a "trojan" program or rooted computer virus that perform destructive unauthorized actions. For example, the recording of information on a foreign media, illegal transmission of communication channels, unauthorized printing of documents, violation of their integrity, unauthorized copying of important information, the value of which is determined and limited for a very short or, conversely, long time.

Threatening is the situation where an intruder is an authorized user of an information system who, in connection with his functional duties, has access to one part of the information, and uses another part beyond his authority. There are many ways the authorized user can disrupt the operation of the information system and obtain, modify, distribute or destroy the information to be protected. To do this, you can firstly use privileged IO commands, uncontrolled authorization or legitimacy of the request, and access to databases and data banks, servers, etc. Free access gives the intruder the opportunity to access other people's files and databases, and change them accidentally or intentionally.

During maintenance of the equipment, the remains of information on its carriers (hard disk surfaces, magnetic tapes and other carriers) can be found out. Erasing information by conventional methods (by means of operating systems, special software utilities) is ineffective in terms of technical protection of information. The intruder can recover and read its remains, which is why one needs only special means of erasing the information to be protected. During trans portation of carriers in the non-protected territory, there is a threat of interception of information to be protected and its further reading by other parties. An intruder may become an authorized user of the information system in time-sharing mode, if he has previously determined the order of operation of the authorized user or if he works with him on the same lines of communication. The intruder can connect to the communication link between the terminal and the computer processor. In addition, without interruption of work of authorized user, the intruder can continue the operation on their behalf by canceling the signals of the disabling of the authorized user.

The processing, transmission and storage of information by hardware means of the information system is provided by triggering logic elements based on semiconductor devices. The elaboration of logic elements is caused by high-frequency displacement of levels of voltages and currents, which leads to the emergence of environment, power and ground links, as well as in parallel-placed links and inductances of foreign equipment of electromagnetic fields that carry the characteristics of the information being processed in the amplitude, phase and frequency of their oscillations the characteristics of process information. Use by intruder of different receivers can lead to unauthorized leakage and interception of very important information stored in the infor-

mation system. With the decrease in the distance between the receiver of the intruder and the hardware of the information system, the probability of receiving such information signals increases.

Conclusion

The complex task faced by modern users of information systems at manufacturing enterprises is to increase the efficiency of its work, namely, a comprehensive action on the production process, interaction with information, network infrastructure, organizational structure, management and payment systems, and the corporate culture of production.

After the analysis of PJSC "Research and Design-Processing Institute of the Enameled Chemical Equipment and New Technologies KOLAN", were given recommendations for the implementation of the following comprehensive security measures for the use of information: physical means; hardware; software tools; hardware and software means; cryptographic and organizational methods.

Physical means of protection are the means necessary for external protection of computer facilities, territories and objects. They are implemented on a computer basis, which are specifically designed to create physical barriers to possible ways of intrusion and unauthorized access to components of protected information systems.

Hardware protection means are a variety of electronic, electronic and mechanical and other devices that are mounted in serial units of electronic processing and data transmission systems for the internal protection of computer equipment: terminals, input and output devices, processors, communication lines, etc. Software tools, built in the software system, are required to perform logical and intelligent security features. Hardware and software means of protection are tools based on the synthesis of software and hardware means.

Organizational measures for the protection of information constitute a set of measures for the selection, verification and training of personnel involved in all stages of the information process.

Therefore, the main aspect in development and practical and safe application of the information system in the workplace, is the introduction of all methods of protection in the field of its information support, which helps the data integrity optimization and savings.

REFERENCES

1. Sievierinov, O.V., Chernysh, V.I. and Molchanova, M.Y. (2011), "Information security management in accordance with international standards", *Control, navigation and communication systems*, CSRI N&M, Kyiv, pp. 250-253.
2. International standard ISO/IEC 27002, available at: www.iso27000security.com.
3. The Law of Ukraine. The protection of information in information and telecommunication system, available at: http://zakon.rada.gov.ua/laws/show/.
4. The greatest and biggest attacks of computers viruses ever, available at: http://tass.ru/info/4248876.

Рецензент: д-р техн. наук, проф. О. Л. Ляхов,
Полтавський національний технічний університет імені Юрія Кондратюка, Полтава
Received (Надійшла) 28.02.2018
Accepted for publication (Прийнята до друку) 30.05.2018

Проблеми комплексного захисту інформації на підприємстві ПАТ «НДІ Колан»

Г. В. Головко, М. Г. Колтунов, А. С. Самофал

Мета дослідження – описати особливості використання систем захисту інформації у діяльності підприємства ПАТ «НДІ КОЛАН». Виявлено сутність систем захисту інформації та задачі, які вони можуть виконувати. **Мета** роботи полягає в тому щоб висвітлити проблему комплексного захисту інформації на підприємствах. Отримано наступні **результати**. Захист інформації виконує чотири важливих функції для організації, захист здатності функціонування організації, забезпечує безпечну роботу програмних додатків, що впровадженні у ІТ системи на підприємстві, захищати дані які збирає та використовує організація, і нарешті, гарантує безпечне зберігання технологічних активів, що використовуються на підприємстві. **Висновки**. Визначено основні складові частини, які утворюють внутрішню та зовнішню безпеку інформацію. Доведено, що використання систем захисту інформації є обов'язковою умовою у діяльності сучасного підприємства або виробництва, що сприятиме запобіганню втрати або викрадення важливої конфіденційної інформації. Доведено, що інформаційна безпека захищає дані від загроз або вірусів. Інформаційна безпека важлива на підприємствах, оскільки може захистити конфіденційну інформацію, забезпечити функціонування організації, а також забезпечує безпечну роботу програмних додатків, які використовують ІТ системи підприємства, та інформаціє важливим активом для організації.

Ключові слова: захист, захист інформації, інформаційна безпека, безпека інформації.

Проблемы комплексной защиты информации на предприятии ПАО «НИИ Колан»

Г. В. Головко, Н. Г. Колтунов, А. С. Самофал

Цель исследования – описать особенности использования систем защиты информации в деятельности предприятия ПАО «НИИ КОЛАН». Определена сущность систем защиты информации и задачи, которые они могут выполнять. **Цель** работы заключается в том, чтобы осветить проблему комплексной защиты информации на предприятиях. Получены следующие **результаты**. Защита информации выполняет четыре важных функции для организации, защита способности функционирования организации, обеспечивает безопасную работу програмних приложений, внедрённых в ИТ системы на предприятии, защищать данные, которые собирает и использует организация, и наконец, гарантирует безопасное хранение технологических активов, используемых на предприятии. **Выводы.** Выявлено составные части, которые создают внутреннюю и внешнюю безопасность информации. Доказано, что использование систем защиты информации является обязательным условием в деятельности современного предприятия или производства, что будет способствовать предотвращению утери или кражи важной конфиденциальной информации. Доказано, что информационная безопасность защищает данные от угроз или вирусов. Информационная безопасность важна на предприятиях, поскольку может защитить конфиденциальную информацию, обеспечить функционирование организации, а также обеспечивает безопасную работу программных приложений, которые используют ИТ системы предприятия, и информация важным активом для организации.

Ключевые слова: защита, защита информации, информационная безопасность, безопасность информации.