METHODOLOGY OF FORMING OF THE PROTECTED INFORMATION SYSTEM OF A TRADING ENTERPRISE

[a]S.E. GAZIZOVA, [b]A.R. GAZIZOV, [c]E.R. GAZIZOV

[a]Kazan Federal University, Bachelor's Degree in Mechanics of liquid, gas and plasma, Master's Degree in Mechanics, 18 Kremlyovskaya street, Kazan 420008, Russia
[b]Don State Technical University, PhD in pedagogy, Ploshchad' Gagarina, 1, Rostov-on-Don, Rostov Oblast, 344002, Russia
[c]Kazan State Agrarian University, PhD in physical and mathematical sciences, assistant professor, st. Karl Marx 65, Kazan, Tatarstan rep, Kazan, Tatarstan, 420015, Russia
email: [a]silmaril92@mail.ru.; [b]gazandre@yandex.ru; [c]gazizov.e@bk.ru;

Abstract. The article discloses a methodology for building a secure information system (IP) of a trade enterprise. Information resources are classified taking into account the peculiarities of the trading activity of the enterprise. Their contents are disclosed. The basic principles of the formation of a protected IP trading enterprise taking into account with the specific activities. The requirements for a secure IP are defined. Recommendations are given for its formation. The purpose and content of the IP security policy are disclosed. The theoretical foundations of the organizational and administrative component and the technical component of the protection system are formulated. The conclusion is drawn on the universality of the presented methodology, which allows for the construction of a secure IP trading enterprise.

Key words: secure information system, basic principles of the formation, IP

1 Introduction

In accordance with the national standard of the Russian Federation "GOST R 51303-2013. Trade. Terms and Definitions "(National Standard of the Russian Federation GOST R 2017), a trading enterprise is a property complex located in a shopping center and outside a retail facility used by trade organizations or individual entrepreneurs to sell goods and provide services to trade. The information resources of a trading enterprise are the totality of all received and accumulated information in the course of practical activity of the employees of the enterprise and the functioning of special devices used in the management of a trading enterprise. The information of the trading enterprise is the data extracted from the business documentation of the enterprise, concerning the sale of goods and the provision of trade services and received from the partners in the order of information interaction, that is, the process of transmitting and receiving information, while enabling the collection, processing, production, archiving, broadcasting information by means of information and communication technologies (ICT) (Robert 2010; Robert 2009). In the trading enterprise, the main sources of information are people (employees of the enterprise), as well as electronic and paper data carriers. At the same time, the number of electronic and paper media in the process of information interaction between users is equal.

2 Methods

We will disclose the classification of information resources of a trading enterprise. The use of paper carriers complicates the operations of collecting information, producing, accumulating, storing, processing and transferring it, but making it less vulnerable to an attacker. Currently, the implementation of software and hardware information protection tools in ICT facilities of a trading enterprise (such as electronic digital signature, firewall and so on) in the process of information interaction of users is not enough. In addition, it is necessary to document the trade operations, so the presence of paper data carriers is still relevant. Taking into account the specifics of the sale of goods and the provision of trade services, the information resources of a trading enterprise are subject to the following classification:

1. Information about customers. This information is stored in the database of the information system of the trading company. This is the data on physical or legal persons who cooperate with the trading enterprise. Access to customer information is limited. Confidentiality of information about customers is due to the fact that its intentional distortion or loss can lead to negative consequences, and in particular to loss of profit by the enterprise. At the same time, under the information system of a trading enterprise operating on the basis of ICT facilities, we understand the system for the transfer and reception of information from a trading enterprise, consisting of a source of information, a transmitter, a communication channel, an information receiver, and a source of interference (Robert 2010; Robert 2009).
2. 2. Information about employees. This information includes personal data of each employee, including passport data, place of residence, marital status, data on the previous place of work, etc. When applying for work, each employee provides his personal data to the staff of the trading company. In doing so, he gives written consent to their processing. After that, a personal file of the employee is entered, which includes his personal data. Personal data is organized and stored in the personnel body of the enterprise. In accordance with Federal Law No. 152-FZ of July 27, 2006 (as amended on July 21, 2014) "On Personal Data" (Federal Law of July 27 2017), this information is confidential. Access to it is available only to employees of the cadre body, as well as persons authorized to do so in accordance with the job description. The main carriers of information about the employees of the trading enterprise are paper carriers. At the same time, there is a named set of data on employees of a trading enterprise in the information system. This means that there is a database that includes key information about employees and is protected by software and hardware.
3. Communicative information. This information provides information interaction between employees of the trading company and external counterparties. This information is freely available (usually on the site of the trading company) and includes the form of ownership and name of the trading company, actual and legal addresses, telephones for communication and so on. This information is not protected.
4. General information. This information includes standard indicators that characterize the activities of a trading enterprise, without taking into account its specifics. This information is freely available and is not subject to protection.
5. Financial information. This information is very valuable for the attacker from a commercial point of view, which implies its reliable protection. This information includes information about the company's accounts, its financial operations, financial assets of the enterprise, employee salaries and etc. Thus, it fully describes the financial condition of the trading enterprise at a given time or a particular period of time. Violation of the integrity, confidentiality and accessibility of financial information can lead to disastrous consequences for the trading company, so do not neglect its protection. Most financial information is stored in digital form and processed with the help of special software, which makes it the most vulnerable and accessible from outside for intruders. Therefore, in the process of information interaction between users of a trading enterprise, the protection of financial information must be given increased attention.
6. 6. Legal information. This information is public and can be disclosed without any negative consequences for the trading company. This information includes the charter of the enterprise, orders regulating the work of the enterprise, memoranda (agreements) on cooperation with external contractors. Thus, these documents are a legal superstructure of the trading enterprise and regulate the internal and external legal relations of the enterprise. Legal information is stored, as a rule, on paper. At the same time,

with the gradual introduction of electronic document management systems, many documents are kept in digital form and signed with the help of an electronic digital signature, which is an analogue of the signature of an individual obtained using ICT tools and cryptographic transformation of information. After expiration of the established period of storage, legal documents are handed over to the archive, where they are stored in the future.

The above types of information have a different degree of significance for the trading enterprise, therefore, have a different degree of commercial and other value to the attacker.

Now we will reveal the principles of the formation of a protected information system of a trading enterprise. Based on the analysis of the possibilities of ICT tools as a means of processing information in the information system of a trading enterprise in the conduct of office work and automation tools for making managerial decisions, and also analyzing the importance of the information resources of a trading enterprise, the construction of a secure information system should be based on the following principles (Gafner, 2010):

1. The principle of continuity is the first and most important. The essence of this principle is the constant control over the security of the information system. In identifying weaknesses, as well as potentially possible channels of information leakage and unauthorized access to the system. And also in updating and supplementing the protection mechanisms, depending on the changes in the nature of internal and external threats, justification and implementation on this basis of the most rational ways of protecting information.
2. The second is the principle of complexity. It proceeds from the nature of the actions of intruders, seeking to extract important information for competition by any action. In this principle, it is legitimate to say that the weapon of defense must be adequate to the weapon of attack.
3. The third is the principle of system. The greatest effect is achieved in the case when all the means, methods and measures used are combined into a single, holistic mechanism, that is, to the information system protection system. Exceptionally in this case, the system properties of information system protection appear that are not applicable to individual elements, and also the ability to manage protection and redistribute resources to ensure the continuous operation of the information system.
4. Fourth - the principle of legality, reasonable sufficiency and professionalism of employees. The most important conditions for ensuring security are lawfulness, sufficiency, respect for the balance of interests of the individual and the enterprise, the high professionalism of employees involved in the protection of the information system, as well as the training of users and compliance with established rules for the protection of information, mutual responsibility of managers and specialists of the enterprise, information interaction with state and law enforcement agencies.

3 Results

Dedicated principles allow to determine the thematic filling of requirements for a protected information system of a trading enterprise (Cheluhin, 2014).

1. The system must be centralized. The management process of the information system is always centralized, therefore the structure of the system implementing the process of its protection should correspond to the structure of the system itself.
2. The system must be scheduled. The planning process is carried out to organize the information interaction of all structural units of the trade enterprise in the interests of implementing the adopted policy of protecting the information system. Each service and department develop detailed information protection plans in the sphere of their competence and taking into account the overall goal of the enterprise (Bahremand, 2015).
3. The system should be specific and focused. Specific information resources, which may be of interest to potential competitors, must be protected.
4. The system should be active, that is, provide protection with sufficient degree of perseverance and purposefulness. This requirement presupposes the presence in the system of protection of forecasting tools, expert systems and other tools that allow implementing along with the principle of "detect and eliminate" the principle of "foresee and prevent".
5. The system should be reliable and universal, that is, cover the whole complex of information activities of a trading enterprise. Methods and means of protection of the information system must reliably cover all possible channels of information leakage and counter ways of unauthorized access, regardless of the form of information, the language of its expression, and the type of media on which it is located.
6. The system should be non-standard in comparison with the information system of other enterprises and diverse in the methods of protection used.
7. The system should be open to change and supplement the measures to ensure the protection of the information system.
8. The system should be cost-effective. This means that the costs of forming a secure information system should not exceed the amount of possible damage.

Along with the principles and requirements, there are recommendations that should be applied when building a protected information system of a trading enterprise:

1. "Mechanisms" for the protection of the information system should be simple for maintenance and "transparent" to users.
2. Each user must have a minimum set of "privileges" required for information interaction.
3. It should be possible to disable the "mechanisms" for protecting the information system in "special" cases, when the mechanisms "interfere" with the information interaction of users.
4. Independence of "mechanisms" of protection from the system itself.
5. Developers of "security mechanisms" should assume that users have the worst intentions, and also that they will make serious mistakes and look for ways to bypass protection mechanisms.
6. Lack of excessive information on the existence of "mechanisms" for protecting the information system.

The system of protection of the information system of the trading enterprise should include two components: administrative and technical.

1. The administrative component is based on a set of internal documents regulating the issues of ensuring the protection of the information system:

a) documents of the first level of the information protection policy, defining the strategic objectives of the management of the trading enterprise in this area;

b) documents of the second level of the policy, including administrative documents regulating the issues of organizing and conducting work to protect the information system;

c) documents of the third level of policy, including executive documentation, job descriptions and documents regulating protection issues.

The administrative component in the construction of a protected information system of a trading enterprise should include the activities performed in the process of creating and operating the system in order to ensure the protection of information. These activities cover all components of the structure of the system, as well as elements of its protection at all stages of the life cycle.

Activities to implement organizational measures in the construction of a secure information system of a trading company relies on the regulatory framework for the protection of information and should include:

a) limited physical access to the elements of the system and implementing measures to ensure confidentiality;

b) limited ability to intercept information from the system;

c) restricted access to system resources by distinguishing between access and using cryptography methods for data transmission;

d) creation of backup copies (including paper ones) of "critical" information;

e) fight against computer viruses;

f) organization and maintenance of access control, control of visitors, security of premises and territory;

g) organization of information protection in the information system, including the appointment of a person responsible for the protection of information at the enterprise, systematic monitoring of personnel activities, compliance with the procedure and rules for accounting, storage and destruction of documents.

Activities to implement organizational arrangements with employees of a trading enterprise should include:

a) job interview;

b) familiarize the employee with the rules of work;

c) employee training in the rules of work;

d) briefing on the need to preserve trade secrets upon dismissal from work.

With a candidate for a vacant seat, an interview is held, after which the question of hiring is decided.

Familiarization of the employee with the rules of work in the information system of the trading enterprise, as well as his training in the rules of work in the system, involves the formation of knowledge and practical skills of work (Gazizov, 2017). And it concerns work with the information representing a trade secret of the enterprise.

Instruction an employee about the need to preserve a trade secret when he leaves his job aims to prevent its disclosure.

The security policy of the information system of the trading company is an organized set of information security tools, methods and activities aimed at ensuring the integrity, confidentiality and availability of the company's information resources.

Security policy is one of the key components of the overall program for protecting the information system of a trading enterprise. Security policy is the political statement in which the initial requirements for the protection of the information system can be formulated.

The security policy of the information system of the trading company should establish:

a) the importance of information, that is, to establish the position of the company’s management on the value of information;

b) responsibility, that is, appoint employees of the enterprise who will be responsible for protecting information in the information system;

c) the enterprise's obligations to protect information in the information system;

d) area of application (segments of the enterprise information system, to which the policy applies).

The security policy after its approval should not be adjusted. For example, the requirement to use a specific package for virus detection, including the name of the package, may be too specific in terms of the pace of development of antivirus programs. It will be more correct to designate that the virus detection software should reside on the personal computers of users, servers and so on, which will allow IT system administrators to determine the specific type of antivirus software themselves.

2. The technical component should include:

a) the anti-virus protection subsystem, which must meet the following requirements: organization of antivirus activity monitoring, organization of two-level antivirus protection with application of antivirus applications of various manufacturers, provision of antivirus protection of server equipment;

b) a backup and archive subsystem that must meet the following requirements: the creation of appropriate documents and instructions (regulating the backup and archive process and related to the production need), the organization of backup for all servers (specified in the backup rules), the development of procedures, regular execution and testing of backup copies;

c) the e-mail protection subsystem, which must meet the following requirements: the use of secure mail exchange mechanisms within the information system; ensure user authentication when sending e-mail;

d) an attack detection subsystem; in order to control and promptly respond to unauthorized operations in the interfacing segment and server segments of the information system, it is recommended to implement an intrusion detection system designed to detect attacks on the nodes of the information system in a timely manner;

e) subsystem of protection of data transmission channels, which will significantly increase the security of information interaction between external counterparties and employees of the trading enterprise;

f) a subsystem of user identification and authentication to centralize the management of authentication information and ensure that the information system conforms to the requirements of the regulatory documents of the Federal Service for Technical and Export Control of the Russian Federation.

4 Summary

The presented concept of building an information system of a trading enterprise is universal. It will allow to ensure the secure functioning of the information system in the implementation of activities aimed at the implementation of the process of sending and receiving information, in the implementation of feedback, ensuring the possibility of collecting, processing, producing, archiving, broadcasting information within the trading enterprise.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

Literature

1. Cheluhin V.A.: Kompleksnoye obespecheniye informatsionnoy bezopasnosti avtomatizirovannykh system [Comprehensive information security of automated systems]. Komsomolsk-on-Amur, KNAGTU, 2014. 207 p.

2. Federal Law of July 27, 2006 N 152-FZ "On Personal Data". System GARANT [Electronic resource]. Available at: http://ivo.garant.ru/#/document/12148567/paragraph/24880:2 (accessed 29.12.2017). (in Russian)
3. Gafner V.V.: Informatsionnaya bezopasnost' [Information security]. Rostov on Don, Phoenix Publ., 2010. 324 p.
4. Gazizov A. R., Gazizov E. R., Gazizova S.E.: Theoretical aspects of estimation of personal characteristics and professional competencies of company personnel. Turkish Online Journal of Design Art and Communication, Volume 7, 2017. 934-940. p.
5. National Standard of the Russian Federation GOST R 51303-2013 "Trade. Terms and Definitions "(approved by the order of the Federal Agency for Technical Regulation and Metrology of August 28, 2013 N 582-st) (with changes and additions). System GARANT [Electronic resource]. Available at: http://base.garant.ru/70795476/#ixzz526vXWdl6 (accessed 29.12.2017). (in Russian)
6. Robert I.V.: Teoriya i metodika informatizatsii obrazovaniya (psikhologo-pedagogicheskiye i tekhnologicheskiye aspekty) [Theory and methodology of informatization of education (psychologo-pedagogical and technological aspects)]. Moscow, Publishing house of the Institute of Informatization of Education of the Russian Academy of Education Publ., 2010. 356 p.
7. Robert I.V.: Tolkovyy slovar' terminov ponyatiynogo apparata informatizatsii obrazovaniya. [Explanatory dictionary of terms of the conceptual apparatus of informatization of education]. Moscow, Publishing house of the Institute of Informatization of Education of the Russian Academy of Education Publ., 2009. 96 p.
8. Bahremand, A.: The concept of translation in different teaching approaches and methods. UCT Journal of Social Sciences and Humanities Research, 3(1). 2015. 5-9 p.

Primary Paper Section: A

Secondary Paper Section: AE, AH