ANALYSIS OF THE PROBLEM OF PROTECTION OF INFORMATION IN THE CORPORATE INFORMATION SYSTEMS SEGMENT

Yegana Novruz Aliyeva, Laman Qadir Ibrahimova
Azerbaijan State Oil and Industry University, Baku, Azerbaijan:
yegane.aliyeva.1969@mail.ru, l.ibrva88@gmail.com
https://orcid.org/0000-0002-4211-9806

Abstract. Successful use of modern information technologies is impossible without effective management of not only the computer network, but also the IT process. Improvement of information security management is possible both by using new methods for solving the management problem and by increasing the quality of the management effect by reducing the duration of these control periods. Therefore, a reasonable approach to increasing the effectiveness of information security measures can be the development of intelligent decision-making tools related to information management issues. Although active research is currently being conducted on the development of IT methods and systems, there are still many unanswered questions about the creation of methods for creating intelligent PPR tools related to IT management, which indicates a need. Complex solutions to scientific problems aimed at developing not only scientifically based, but also practically applicable models and methods for intellectual support of IT process management.

Keywords: *data, standard, information technology, operation, Fast Ethernet.*

Introduction

Modern corporations have a complex distributed structure, predetermined by multifaceted activities, territorial location of divisions, and numerous corporate relationships with partners. Corporate management systems are usually called enterprise management systems that have a developed structure and separate management bodies. Corporate systems include organizational, information, etc. Most business functions and management processes of enterprises and organizations involve corporate information systems (CIS), which are essential tools for conducting business. The introduction of new information technologies for enterprises is always associated with the emergence of new risks. The more complex the structure of the corporate information system, the higher the risk of threats to it: penetration from the outside or unauthorized access from within the enterprise, especially for the purpose of financial fraud or disclosure of commercial secrets, changing or destroying information. and so on. [1, p. 147-153] Such risks can seriously damage the enterprise. The creation of a developed and secure information environment is an indispensable condition for the development of both individual corporations and the economy, society and the state as a whole. Therefore, the issues of ensuring information security in the CIS segment have become very urgent now.

CIS is a complex human-machine or socio-technical system that integrates the enterprise's information system. Different types of models are used to study such systems. The operation process of the CIS enterprise is carried out in the conditions of conflict between the enterprise as a socio-technical system on the one hand and competitors, aggressors, negative natural phenomena and other objects and events on the other. The complexity and expansion of modern corporate information systems leads to an increase in the number of network devices and various information security tools (ISI), and a large number of security incidents. It should be noted that modern technological processes in the field of information technologies, as well as in the field of new communication opportunities, are far ahead of the theoretical understanding of practical developments and applications. Therefore, there are reasons to assume that the current theoretical achievements are not fully adequate to the challenges of information security, both from a practical and a theoretical point of view [2, p. 225-230].

The main drawbacks of widely used information security systems are their strict architectural principles [3] and the use of mainly defensive or offensive strategies to protect against the most known and dangerous threats. Solving the identified problems and effectively using the modern CIS requires equal and reliable management tools and methods of not only networks, but also the security system and all measures that ensure network security. By managing both network and security equipment, we need methods that allow us to quickly monitor changes in the system's operating environment and prevent information security breaches in a timely manner. A modern approach to ensuring effective information security in a corporate information system is the use of intelligent decision support tools (DSS) for information security management.

Experimental part

Currently, an integrated information management system is being developed, which will cover the entire infrastructure of the organization and will allow managing the information infrastructure regardless of the scale of the corporate information system.

A structured description of all aspects of information security management is clearly shown in Fig. 1.

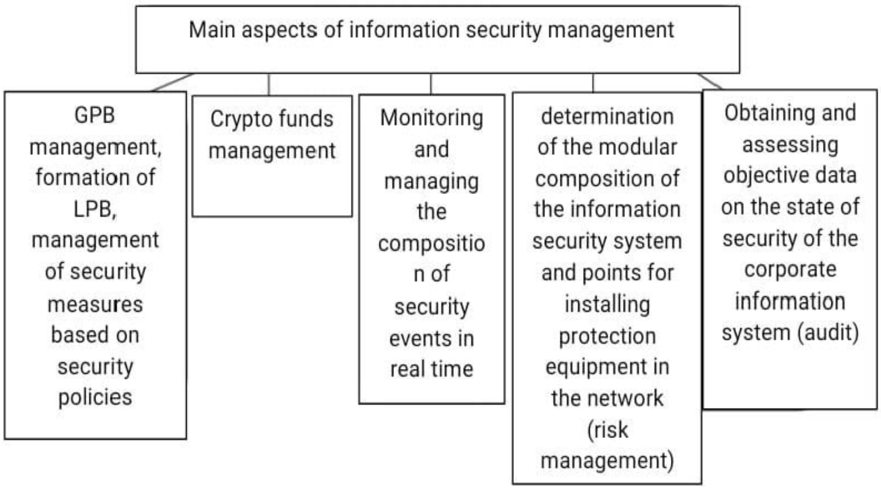
Main aspects of information security management
GPB management, formation of LPB, management of security measures based on security policies
Crypto funds management
Monitoring and managing the compositio n of security events in real time
determination of the modular composition of the information security system and points for installing protection equipment in the network (risk management)
Obtaining and assessing objective data on the state of security of the corporate information system (audit)

Fig. 1. Structuring the property management problem

Currently, it is practically impossible to find manufacturers that will provide the consumer with the full range of both hardware and software necessary to build information security systems that meet modern requirements. Most IT systems are based on software and hardware produced by different manufacturers. To ensure the reliability of the heterogeneous CIS of information security, an Information Security Management System (IMS) is required, which can ensure the correct configuration of each of its components and automatically support decision-making related to information, which can constantly monitor changes and monitoring the work of network users.

Such an integrated approach to solving the problem allows creating a truly safe environment for the operation of the CIS enterprise. Our analysis allows us to confirm that the management system, which performs a number of management functions at the CIS segment level, should work autonomously:

– Obtain and evaluate objective information about the current state of CIS security (audit);

– manage said events;

– determines the modular composition of the information security system and the points of creation of information security tools in the computer network of the enterprise.

The international standard ISO/IEC 27001 describes the models used for the creation, implementation, operation, continuous monitoring and analysis, maintenance and improvement of information security management systems (IMS) [4]. The design and implementation features of the company's information security system are determined by its needs and goals, security requirements, and the size and structure of the organization. Different activities need to be defined and managed in order to function effectively. The process approach to property management in this standard helps to emphasize the following points:

- Establishing appropriate principles, objectives, processes and procedures improving risk management and business intelligence to drive results, is consistent with the company's goals;

– Implementation and operation of IBS rules, controls, processes and procedures;

– assessment and measurement of process indicators related to information security management policy, goals and practices and their analysis;

– implementation of corrective and preventive procedures based on the results of internal audit and analysis in order to continuously improve the management of proprietary information.

The composition of SMZ includes:

– organizational structure;

– policy, planning activity;

– a set of procedures, processes, resources.

The purpose of the information protection system is the design of information protection systems, implementation, operation, continuous monitoring, analysis and improvement of information protection systems.

To create an IBS, an enterprise must:

– determination of system boundaries;

– develop the principle of action related to information protection, taking into account the legislative norms and the established protection goals;

– develop criteria for assessing the importance of risks;

– choose a risk assessment methodology that is compatible with the proprietary information management system and meets regulatory requirements; and able to ensure that risk assessments produce concrete results;

– determine the acceptable level of risk;

– identify risks (assets, threats and adverse effects leading to loss of confidentiality, integrity and availability of assets and critical vulnerabilities of the deployment system);

– assess the importance of risks (assess the possibility of information security violations, taking into account existing threats and vulnerabilities, assess risk levels, determine whether risks are acceptable or whether countermeasures should be taken);

– finding opportunities for risk management (using acceptable means to reduce or accept risk);

– choose risk management and treatment methods that take into account risk acceptance criteria;

– Agree with the management on the implementation of the IT system and prepare a statement on the degree of applicability (including the purpose of control, control tool, justification of choice).

The stage of implementation and operation of the SMPS of the enterprise includes the following actions:

– formulation of a risk management plan that defines the appropriate management measures, required resources, and responsibilities;

– implementation of this plan, including financing;

– implementation of control aimed at achieving the purpose of control;

– implementation of procedures and other management tools capable of quickly detecting events occurring in the information security system and reacting to an incident occurring in the information security system;

– rapid identification of ongoing and completed IT violations and incidents;

– detection of incidents in the information security system and prevention of incidents using indicators;

– measuring the effectiveness of control measures to verify that requirements are met;

– updating information security plans to take into account information obtained during both ongoing monitoring and analysis activities.

IBS documentation should be prepared in such a way that it includes descriptions of risk assessment methods, risk treatment plans and procedures necessary for the enterprise to ensure effective planning. The ISO/IEC 17799 standard provides recommended guidelines to be used when designing a security system. The standard provides a management objective and a list of management tools. The purpose of the security policy is to guide and support the management of the IT in accordance with business requirements and legal regulations. IT policy should be reviewed at scheduled intervals to ensure adequate compliance and adequacy.

When it comes to asset management, the goal is to provide and maintain the necessary means to protect an organization's assets in a business environment that requires clear definition. It is necessary to create and maintain registers of important assets, as well as assets that are in any way related to information processing tools. Information should be classified according to its importance and criticality to the company.

The roles and responsibilities of employees and users regarding information and its protection should be documented in accordance with the company's information policy.

The goal of network security management is to protect security information on networks and protect the network infrastructure. Adequate network management is required to protect against risks. The purpose of continuous monitoring is to determine the information processing activity. A procedure should be established to continuously monitor the use of the tools used to process data and the results should be regularly reviewed.

The purpose of user access control is to guarantee access to registered users and to prevent unauthorized access to CIS. The assignment and use of permissions should be controlled and restricted, and the assignment of passwords should be governed by a formal administrative process. A formal user registration process should be established.

The purpose of information security incident management is to ensure that events in the information security system and vulnerabilities in the information security system are reported in a way that allows for timely correction processes. It is necessary to define management tasks and procedures for prompt, effective and organized response to all incidents that occur in the information security system. In the information security system, it is necessary to provide a mechanism that allows to determine the number and volume of incidents and constantly monitor them.

In [5, p. 120-121], a model of management process maturity is presented information security, in which the highest levels are “managed” and “optimized”. The controlled level is characterized by the evaluation of the monitoring and control process in the protection facility, their optimization is carried out, automation tools are partially used. The level of optimization characterizes the complexity of the information security management process, the ability to quickly adapt during changes in the business process, and the comprehensive use of protection measures that provide a basis for improving management processes.

The main steps to be followed include the information security management process [1, p. 220-227]:

– planning - analysis and assessment of information security risk, determination of policies on information security management systems, selection of protection measures and their updating to minimize risks, making decisions regarding the application of the information security management system;

– implementation and operation of the information security management system, including the development of plans for the processing of information security risks, the implementation of measures for its protection, work management, the detection and response of emerging security incidents;

– verification (monitoring and analysis), including analysis of activity, including analysis of residual information security risk levels, analysis of internal audits of the information security management system;

– improvement of the IS management system, including implementation of tactical and strategic improvements in the system, assessment of goal achievement, requiring decision-making at the planning level.

The ISO/IEC 15408-2002 standard includes security management steps; is a guide for security management in the information and communication system.

The standard covers general management issues important to the effective planning, implementation, and maintenance of system security.

Analysis of existing security management standards concluded that they try to create common concepts and common models for security management; however, these standards do not include specific approaches to information security management in SG CIS.

CIS of modern companies is an important tool for business management and an important means of production. The structure of the CIS consists of two large blocks:

– information infrastructure;

– information services.

The information infrastructure block represents the material base and environment for information service activity. The infrastructure of a modern company and modern society can be represented as consisting of spatially distributed units of this society and its partners, customers and suppliers. The main interactions between the company's facilities are carried out within the framework of the distributed CIS using communication devices and communication channels assigned by the telecommunications operator using various network programs and services.

The main principle of the structure of the distributed CIS is the segmentation of the network according to the territorial production affiliation. CIS structural units are a distributed segment of CIS. The CIS segment, in turn, can be a complex information system distributed at the regional level.

A CIS segment is a network consisting of network segments of the second level of the hierarchy. Each segment has a network built on workstations, servers, routers, a set of switches, digital modems, telephone lines, Fast Ethernet, E1 fiber optic channels and wireless communication channels.

The problem of ensuring information security in the corporate information system can be solved by establishing an effective information security system.

On the fig. 2 SG CIS clearly demonstrates the model of the composition of the information protection system.

The IT system is subject to the requirement of absolute transparency for programs already existing within the CIS and, in addition, to the requirement of compatibility with the network technologies used by the corporation. Therefore, in order to ensure reliable protection of CIS resources, information security systems should be implemented based on the most advanced and promising technologies in the field of information security.

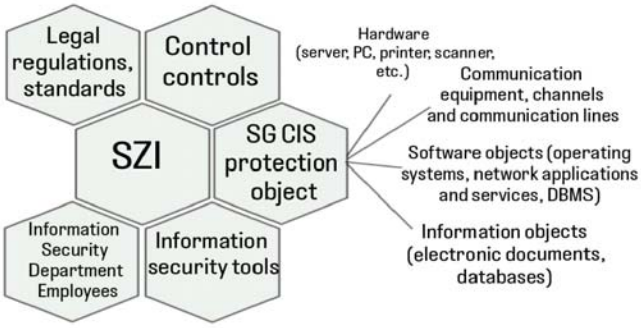
Legal regulations, standards
Control controls
SZI
SG CIS protection object
Information Security Department Employees
Information security tools
Hardware (server, PC, printer, scanner, etc.)
Communication equipment, channels and communication lines
Software objects (operating systems, network applications and services, DBMS)
Information objects (electronic documents, databases)

Fig. 2. SG CIS information security system composition model

Therefore, in order to ensure the effectiveness of computerization in the corporation, it is necessary to ensure the security parameters of information resources such as the integrity, confidentiality and authenticity of relevant business information circulating in local and global information networks.

Conclusion

1. Implementing proactive information security strategies requires complex decisions that include developing a method to assess suspicious activity and various network events, preparing information to make decisions about managing security services and network devices, and responding in real time to changes in operating environment conditions.

2. One of the main problems in creating property management systems is the problem of providing automated decision support regarding property management throughout the entire period of CIS operation and in the changing conditions of the information environment. For this requires infrastructure software that supports mathematical models and scientific decision-making methods. The creation of instrumental software systems that use all the capabilities of a computer will make it possible to make scientifically based decisions, since the decision-making process will be based on analysis and forecast made using mathematical methods.

REFERENCES

1. Застрожнов И.И., Рогозин Е.А., Багаев М.А. Методологические основы безопасности использования информационных технологий в системах электронного документооборота: монография. – Воронеж: Научная книга, 2011, 252 с.
2. Стенг Д.И. Секреты безопасности сетей. – К.: Диалектика, 1996. 544 с.
3. Бородакий Ю. В. Интеллектуальные системы обеспечения информационной безопасности: материалы конф. // Известия ТРТУ. Тематический выпуск. – Таганрог: ТРТУ, 2005. № 4. с. 65- 69.
4 ISO/IEC 27001 – «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью». М.: ФГБУ "РСТ", 2022.
5. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002, 656 с.

Accepted: 06.03.2024