УДК 330

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. В. Скрипко, Д. А. Гармидарова
Научный руководитель – Н. В. Фомина

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: daniilskripko@mail.ru

Чтобы получение информационных услуг было гарантированно возможным, необходимо обеспечить информационную безопасность информационно-телекоммуникационных систем. Компании важно выявить все существующие и реально реализуемые угрозы информационной безопасности. Минимизировать возможность возникновения угроз призваны политики информационной безопасности.

Ключевые слова: информатизация, информационно-телекоммуникационные системы, информационная безопасность, угрозы информационной безопасности, политика информационной безопасности.

INFORMATION SECURITY POLICY

D. V. Skripko, D. A. Garmidarova
Scientific supervisor – N. V. Fomina

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarskii rabochii prospekt, Krasnoyarsk, 660037, Russian Federation
E-mail:daniilskripko@mail.ru

Information security of information and telecommunications systems must be ensured in order to guarantee the availability of information services. It is important for the company to identify all existing and realizable threats to information security. Information security policies are designed to minimize the possibility of threats.

Keywords: informatization, information and telecommunications systems, information security, threats to information security, information security policy.

The global informatization of the modern post-industrial society has led to the fact that corporate information and telecommunication systems, whose task is to obtain specific information services by users, have acquired the most important importance in the conditions of the modern world. However, in order to ensure that the receipt of information services is guaranteed, it is necessary to ensure the security of these systems. This is where the concept of information security is introduced – the protection of information systems and supporting infrastructure from accidental or intentional impacts of a natural or artificial nature, fraught with damage to the owners or users of information resources and supporting infrastructure [1].

There are cases when it becomes impossible for entities with access rights to receive information services. This implies one of the most important principles of information security - ensuring the availability of information. In addition, access to information services should not be carried out by entities that do not have the right to do so. There is another principle – ensuring the confidentiality of information. It is important that any change in information is carried out only intentionally by the

subjects who have the right to it. There is also a third principle - ensuring the integrity of information. In the context of this article, the information security system in the corporate system will be considered as a set of organizational measures and technological solutions that are aimed at ensuring the availability, integrity and confidentiality of information.

Today, any modern promising company should be prepared for the fact that its activities will be closely monitored by competitors who want to intercept information about plans, profitable deals, high-quality and at the same time cheap products, i.e. information that can lead to serious damage to the reputation and financial losses of the company.

It is important for the company to identify all existing and realizable threats to information security, to analyze their potential for implementation.

Threats to information security can be divided into two types:

1. Natural, i.e. not related to human activity:

a) Epidemics, earthquakes, fires, floods;

b) Man-made (an accident at power plants with a power supply interruption due to equipment failure, a pipe break due to material wear);

2. Artificial, i.e. directly related to human activity:

a) Unintentional (accidental entry into a protected object from ignorance of the location of this object);

b) Intentional (arson of a building, introduction of malicious software in order to collect information, leakage of information organized with the help of company employees motivated by personal interests).

But still, most of the risks are associated with the actions of employees who are easily bought by competitors. Information security policies are designed to minimize these risks – sets of measures, rules and principles that employees of the enterprise follow in their daily practice in order to protect information systems. The risks of information leakage of a large company are not comparable to the risks of data leakage at a power plant. Therefore, everything should be taken into account, starting from the channels of physical data transmission (it is unacceptable to use phones with video cameras and Internet access) and ending with the ways of movement of industrial waste.

An important aspect in the development of information security policies is the balance between the costs of information security and possible damage in the implementation of the threat, as well as the likelihood of the threat [2, p. 3].

A well-developed information security policy is a complex hierarchical system of documents, which typically consists of three levels, in which each lower-level document follows from a top-level document and is designed to solve its specific range of tasks. Let's consider the list of documents to be developed at each specific level.

1. Upper level. At this level, one document is adopted and approved by the company's Board of Directors, the task of which is to demonstrate the general attitude of the company's management to the importance of information protection. This document becomes the business card of the company: the availability of high-quality information security standards guarantees contracts with new partners, and especially with foreign ones, for whom stability and reliability of business relations are important. Although the document is declarative and motivational in nature and does not describe specific actions, but its development is important and necessary.

2. The main level. At this level, from one to several dozen documents can be developed and adopted. It is these documents that regulate the actions of specific employees and make it possible for them to be held responsible for non-compliance with the information security policy. Many companies limit themselves only to the list of information that is a trade secret, while others regulate everything – from the mode of copying documents to topics that are allowed to be discussed on corporate phones. The responsibility of employees is based not only on methods, but also on the norms corresponding to them in employment contracts and job descriptions, because only this can become the basis for compensation in court for the damage caused to the company.

3. Technical level. At this level, short manuals are being developed for familiarization by employees, and appropriate changes are being made to employment contracts. This level is a way to inform employees about their responsibilities in the sphere of information protection. And the priority in the development of these documents should be the personalization of responsibility.

When creating documentation, it is important to rely on the following requirements:

1. Lower-level documents must fully comply with the policy of upper-level documents, federal laws, recommendations and standards of regulators in the field of information security (Federal Service for Technical and Export Control, Federal Security Service, Ministry of Defense, Foreign Intelligence Service, Ministry of Communications and Mass Communications);

2. All provisions, instructions, recommendations should be unambiguous, none of the norms should not have a double meaning;

3. The information security policy should fully correspond to the level of training of those employees for whom it is intended. The exchange of information should be differentiated, each employee should follow their own standards, be responsible for their own specific range of tasks.

The protected information is a serious value, for the possession of which many competitors will fight, therefore, only the development of a documentation system will not solve the problem of protecting valuable information, it is necessary to test the system in practice, audit the quality of tasks and, if weaknesses are identified, refine the system, improve it.

Companies that are really willing to spend time and money on the creation, subsequent implementation and further improvement of information security policies can be fully confident in protecting their interests, the interests of employees and customers. Only a well-developed documentation system will be the guarantor of information security.

References

1. Galatenko V. A. Fundamentals of information security. M., 2004. 264 p.

2. Jealous A.V., Fedotov A.M. Review of information security policies. Novosibirsk, 2012. 14 p.