Shcherbina Oleksiy

ENSURING INFORMATION SECURITY OF THE ENTERPRISE

The pace of development of modern information technologies is significantly ahead of the pace of development of the advisory and regulatory framework of the governing documents that are in force today. Therefore, the solution to the issue of developing an effective information security policy in a modern enterprise is necessarily associated with the problem of choosing criteria and indicators of security, as well as the effectiveness of the corporate information security system. As a result, in addition to the requirements and recommendations of the standards, a number of international recommendations have to be used. This includes adapting to domestic conditions and putting into practice the methods of international standards, such as ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL and others, as well as using information risk management methods in conjunction with estimates of the economic efficiency of investments in ensuring the protection of enterprise information. Modern methods of risk management make it possible to solve a number of tasks of the long-term strategic development of a modern enterprise.

First, to quantify the current level of information security of the enterprise, which will require the identification of risks at the legal, organizational, managerial, technological, and technical levels of information security.

Secondly, develop a security policy and plans to improve the corporate information security system to achieve an acceptable level of security for the company's information assets. To do this, it is necessary to: justify and calculate financial investments in security based on risk analysis technologies, correlate security costs with potential damage and the likelihood of its occurrence; determine the functional relationships and areas of responsibility in the interaction of departments and persons to ensure the information security of the company, create the necessary package of organizational and administrative documentation; ensure the maintenance of the implemented protection complex in accordance with the changing operating conditions of the organization, regular revisions of organizational and administrative documentation, modification of technological processes and modernization of technical means of protection.

The solution of these tasks opens up new opportunities for managers of different levels. This will help senior managers objectively and independently assess the current level of information security of the company, ensure the formation of a unified security strategy, calculate, agree and justify the necessary costs for protecting the company. Based on the assessment obtained, the heads of departments and services will be able to develop and justify the necessary organizational measures. Middle managers will be able to reasonably choose information security tools, as well as adapt and use in their work quantitative indicators for assessing information security, methods for assessing and managing security with reference to the economic efficiency of the company.

Practical recommendations for neutralizing and localizing the identified system vulnerabilities, obtained as a result of analytical studies, will help in working on information security problems at different levels and, most importantly, determine the main areas of responsibility, including material, for the improper use of the company's information assets.

The work was carried out under the guidance of Associate Professor of the Department of Marketing and Trade Management T. Obydiennova