ECONOMIC ASPECTS OF ENTERPRISE INFORMATION SECURITY

Havrys O.O., Pikalova Y.Y.

National technical university «Kharkiv polytechnic institute», Kharkiv

Types and content of data storage depends on the specifics of the organization. Masses of information contain personal, corporate and confidential information, so theft can lead to catastrophic consequences for an enterprise, both financially and in reputational terms. In addition to storage, modern archives allow timely reporting and analysis of their contents, and database hacking can be carried out both for information corruption and unauthorized access. Both aspects are extremely undesirable and cause a number of consequences. Information leakage is considered one of the main threats to the stability and competitiveness of the enterprise. In order to promptly take measures that reduce the level of risk, that is, the possibility of data loss or damage, it is necessary to study current threats, analyze the feasibility of countermeasures, and take a comprehensive approach to cyber protection of data warehouses. Database security must cover hardware, software, personnel, and the data itself. A database is an important corporate resource that must be properly protected against the following potential threats:

- data theft and falsification;
- breach of confidentiality;
- violation of the integrity of personal data;
- loss of data availability.

These situations indicate the main areas in which management should take actions to reduce the degree of risk, that is, the possibility of data loss or damage. In some situations, all these aspects of data corruption are closely related, so activity aimed at compromising the security of a system in one direction often lead to a decrease in its security in all others. The need for data protection has often been overlooked in the past, but is becoming increasingly apparent to organizations today. The reason for such a change in attitude is the cases of destruction of computer stores of corporate data, as well as the realization that the loss or simply the temporary absence of this data can negatively affect the efficiency of the enterprise. Consequence of the violation of the protection system, which caused the loss of data confidentiality, can be the loss of a reliable position in the competition, and the loss of data integrity will lead to its distortion or destruction. Many organizations operate 24/7, so a loss of availability means that the data or system, or both, will be unavailable to users, potentially threatening the financial health of the organization.

Thus, the goal of database protection is to minimize losses caused by unforeseen events. As the level of online crime has increased significantly in recent years and is expected to continue in the future, it is clear that the effective operation of the enterprise can only be ensured by taking the necessary information protection measures.