THREATS TO INFORMATION SECURITY OF THE ENTERPRISE

Igor Zakharov
Sumy State University, Sumy, Ukraine

Inalienable part of the new economy is information technologies (IT) introduction and application in the all spheres of human activity.

The permanent improvement of present information-communication technologies (ICT) and their application expansion are the part of strategic decisions and operative tasks for enterprises. But every decision-making about the ICT improvement necessity runs into questions about the necessary and sufficient level of improvement, about the financing of this level, about IT-decisions optimization and co-ordination, about defense facilities application of enterprise information base, about necessary and sufficient level of the information safety system expenses. Thus, every company faced such problems as: information safety threats estimation, sooner or later, determination of ICT optimization directions and information system efficiency increasing.

For the picture of possible harm which is inflicted normal activity of the unguarded information system of enterprise, let's consider every threat factor and possible losses which it brings an enterprise. In the general view of threat reliability appear under the action of two kinds of factors: Hardware-factor and human factor.

Hardware-factor. Factor is related to the equipment malfunction. Some time is expended on the error removal: for diagnostics of derangement, block replacement or repairing, new block options and tuning, renewal of user data and settings. I.e. expenses on capacity renewal present the payment for this time and cost of necessary repairing parts.

In respect of human factor, its influence can be related to the intentional and unintentional harm.

Unintentional harm. This factor is related to human influence on the automated system, which can inflict harm an enterprise. Wrong use, non-fulfillment of equipment exploitation rules, employees incompetence, and also other actions, which negatively influence the work of ICT, can result in the temporal uncapacity of the enterprise information system. The removal expenses will be required on failure diagnostics, information base renewal, if it is necessary, and employee teaching for prevention of failure reiteration.

The intentional harm is divided by a few types of information safety threats:

1. *Piracy*. This factor threatens only to those enterprises which activity is connected with the software production and sale, as an independent product, or as inalienable part of the product (for example, the device control program). Inflicted loss will be expressed in the lost profit from the unrealized units of production. Basic estimation complication of loss consists of determining the amount of the unsold copies.

2. *Virus danger*. Viruses can violate work of the separate programs, destroy user files or databases, change or delete system files that will result in the loss of the system capacity and the separate types of viruses can put an equipment out of action. There are not the anti-virus systems, capable on 100% to protect a computer. In the case of defeat, harm can be different – from facetious reports, appearing on the screen of monitor, to the physical damage of equipment because of the devices parameters changing. Also viruses create a threat confidentiality of information on occasion, getting access to the files stored on a computer.

In the case of defeat the virus of the information system of enterprise, it is necessary to expend time on a search and delete the virus, renewal the information, software and operating system. At the first case of defeat it is necessary to study the virus action for the analysis of all the possible consequences of virus defeat or threats. It is also necessary to expend time on diagnostics and treatment other computers of enterprise intranet, as a virus could spread on them.

3. *Spam*. This factor is related to undesirable, publicity or carrying knavish character distribution on information channels. More frequent than all it touches an e-mail. Electronic addresses, indicated in advertising of enterprise, and also addresses which are actively used for a long time, are especially subject to the problem of spam. The use of antispam-filters does not decide a problem completely, and often results in the useful correspondence loss. Thus, it is necessary to expend time for filtration of mail.

Harm from a spam consists of time, expended an employee (if handling of incoming mail is included in their duties) on spam-letters viewing and deleting. The change of electronic address can be required on some cases that will bear additional expenses. Also a spam strengthens a virus danger, as considerable part of spam-letters contains viruses. For more exact estimation of this factor it is necessary to conduct additional research including questioning of employees for determination, whether there is a problem of spam on an enterprise or not, how many employees does it affect and what harm inflicts. It will demand additional temporal expenses, which must be counted for the efficiency estimation of the ICT-using on the enterprise, actively using electronic channels (for example, e-mail) for data transfer and communication.

4. Espionage. This factor is bound by the possible information loss and by its subsequent use, which can result in unfavorable and unforeseeable consequences for the enterprise. Therefore while strategy development of the information system defense it is necessary to foresee expenses on setting of individual passwords for entrance and database access for every employee, control systems for actions and changes in the information base of enterprise etc.

Enterprises must spare enough attention for all aspects of the ICT-use, in order to know about the threats information safety in time. Insufficient attention to this problem often creates barriers for the effective development of the whole business and information infrastructure work in particular.