Ekaterina Romanenko
D.S. Timofeev, scientific supervisor
M.L. Isakova, language adviser
SHEI “National Mining University”, Dnipropetrovsk

Methods and Means of Training Personnel on Information Security

According to studies, more than 80% of incidents in enterprises in which the guilty employees are the result of unintentional actions. Employee participation in matters of information security can both improve the security of the company's assets, and have a positive effect not only on the interaction of staff within the company but also on relations with its counterparts. Staff competence in matters of information security, the ability to apply these skills and knowledge in core business significantly increase the confidence of customers and partners, and contribute to a more stable relationship.

The purpose of training is building and maintaining the necessary level of staff competence, subject to the company in the field of information security and ensuring a high level of security in the information system. Policy objectives of the enterprise in the field of training on information security are:

1. development of and adherence to the rules on data protection;
2. development and implementation of the education system, including the identification of training needs, planning and budgeting, training and monitoring of its effectiveness;
3. construction of training in accordance with the business processes;
4. formation of educational standards;
5. incorporation of best practices, knowledge, and effective methods of work organization in the training of information security;
6. motivating employees to improve safety and ensure reliability;
7. regular testing of knowledge in information security and their application in practice.

Employees’ awareness program implements process of regular upgrading of knowledge employees in information security.

Basic requirements which must satisfy the above solutions:

1. provide the ability to regularly train any number of employees, regardless of their territorial location and workflow;
2. provide data to users in a simple and understandable form;
3. value of all the implemented solutions should be adequate, and should not be directly dependent on the number of students.

Based on the above requirements, it is clear that it is not appropriate to consider full-time training as a method of raising awareness of the regular staff in the IS from the economic point of view. Various corporate e-learning and certain "non-standard" solutions are much better.

The primary means for training a large number of employees at the moment, of course, are a variety of distance learning system (DLS). It is clear that the DLS was not so much a tutorial, but a means of delivery to the end-user information (teaching). Therefore, when choosing DLS usually attention should be paid to two parameters: the basic functional (management of employee training, flexibility, reporting, etc.) and a set of training materials that are provided with the system.

"Non-standard" training employees in information security refers to the different methods and tools that are generally not used for learning - on emotional and subconscious level employee remembers learning material requirements and the importance of information security. Some of the methods of this training are:

Screensavers;

Movies, cartoons, videos;

News by IS;

office supplies.

One example of an appraisal of the practical, rather than theoretical knowledge of the staff is the use of social engineering, when simulating a situation in which the actions of an illiterate person may violate the IS.

To sum up, teaching the basic rules of information security employees of the company and, in particular, using this knowledge in practice, significantly reduce the risk of information security breaches and, consequently, reduce the possible damage the company. In this case, training of employees in information security with the right approach will not be very expensive and time consuming.

Currently, there are many different methods to increase staff awareness in information security. The greatest efficiency, of course, is achieved with the integrated use of different methods.