UDC 004.415.2:371.3

Andy David,
principal consultant, A2D Consultancy Ltd (Essex, United Kingdom)

Yurii Horelov,
Ph.D., associate professor of information technologies and cybersecurity chair of Kharkiv National University of Internal Affairs

Olexandr Horelov,
graduate student of Kharkiv National University of Radio Electronics

Some aspects of security in adaptive systems of distance learning

Distance Learning (DL) is an educational service delivery system that involves the widespread use of new information technologies to enable students to access educational resource, to interact and engage actively with teachers and colleagues while working with educational material. The capabilities of computer-aided presentation and information technology, as well as networked telecommunication technologies, can improve the quality of learning and create a comfortable environment for students as they have the ability to adjust their work with the material according to their current level of knowledge, needs, capabilities, skills and cognitive parameters of personality.

One of the ways to solve the problem of increasing the DL effectiveness is to develop educational Web courses that realize the principles of adaptation and interactivity. The implementation of adaptability provides a means to take into account the individual characteristics of the user (level of knowledge, goals, needs, cognitive characteristics, etc.), to plan the learning process, and offer them the most appropriate educational material in the most suitable form. An application with a high level of interactivity will allow the implementation of more productive scenarios of user interaction with the system, with the study material, and with colleagues.

Advantages of adaptive learning systems include:

- differentiation and individualization of training;

- optimization of the learning processes and knowledge assessment based on prognostic analysis;

- accounting for any previous level of knowledge;

- regulation of the course content by the degree of difficulty;

- students, themselves, define their own learning path, as the real-time response on process of working with the study course provides detailed feedback for self-improvement;

- adaptive systems encourage students' interest in learning through automated feedback cycles, encouraging them to take action and move forward regardless of the course teacher;

- adaptive systems increase the capacity of the teaching staff; a rich analysis of data on student performance allows teachers to constantly improve the course.

However, the spread of DL is not possible without solving a number of problems, one of which is information security. Information security in this context can be considered in two aspects:

1. Ensuring confidentiality, integrity and readiness of information in the learning process.

2. Protecting students from inaccurate, distorted and harmful information.

In the first case, we are dealing with the technical problem of protecting information from the following threats: unauthorized access to digital content, breach of integrity and inadequacy of training resources, disruption of the normal functioning of services and resources, breach of security of testing procedures, as well as unauthorized access to personal information.

A comprehensive approach to the solution of the problem of information security in the DL involves the implementation of a number of procedures. It uses the registration and authentication of the user, the implementation of access control, monitoring and detection of intrusion, the protection of network communications, and the protection of digital data storage.

Security is of particular importance for adaptive learning systems, since in this case it is possible to gain unauthorized access to a student's personal characteristics that are used to construct his model and implement an adaptation mechanism. Usually, the student model contains information about his level of knowledge, hierarchy of learning goals, cognitive, mental and psychological characteristics of the individual. This significantly increases the risk of continued use of social engineering technologies to commit illegal acts.

The second problem – protecting the user from malicious content – has become especially relevant with the advent of the Web 2.0 concept, which significantly changes the model of user interaction with the network. The main features of the new concept include syndication, socialization, collaboration, interactivity and openness. The Internet becomes a means of interaction and communication, community building, and the realization of accessibility to the full range of services in the learning process, rather than just an instrument of access to the learning resources.

Blogging and microblogging, social networking and social presentation systems, wiki projects, social bookmarks, multimedia dissemination systems, shared editorial systems, syndication and notification technologies and more are available to the user.

In these circumstances, the solution to the problem of information security depends largely on media education, professional competence of the teacher, analysis, selection, preparation and systematic verification of information and educational resources, organization and management of student interaction. The teacher should be able to implement pedagogical technologies by means of information and communication technologies, ensuring the integrity and effectiveness of the learning process.

Одержано 21.10.2019