INFORMATION SECURITY OF DISTANCE LEARNING

Konstantin ARKHIPOV and Vasiliy OVODKOV

In the beginning of the 21st Century, an educated person may feel protected only when his or her social status and rights are guaranteed. A person knowing his rights and standing up for them is able to react flexibly to changes in life. In this context, distance learning may be used for continuous education, thus contributing to the personal security. It allows to organize continuous education for almost all social groups. The development of world-wide cooperation makes distance learning independent from users' location. Related projects not only equip one with new knowledge but also open new horizons in self-education and make a participant understand the need for continuous learning. Besides, distance learning provides an opportunity to use different information sources. The current state of information technologies and their development allows us to consider international educational projects that will be able to establish a direct connection between a tutor and a learner and, thus, implement a genuine feature of traditional full-time tuition. Moreover, through international projects one may discuss different concepts; this is especially important for topics such as international security problems, combating terrorism, and building community to develop common strategies.

At present, distance courses on these problems are widely worked out by leading military educational institutions. The weak point of such courses is that they are created independently and without connection to each other. To solve the problem of international security, it is necessary to set some collaboration not only in the military sphere, but also in education and culture. It is important to provide examples of collaboration at the early stages of new knowledge acquisition.[1] One should take into account the fact that present-day students tomorrow will protect our society from terrorism. So, collaborative efforts in establishing international programs and courses are the first steps towards the international collaboration and creation of institutions working at security problems and combating terrorism. However, first of all it is

necessary to solve several organizational problems. The list of issues depends on educational, technological and legal situation in a particular country. Distance courses for military institutions where it is impossible to disclose secret information may serve as an example. Therefore, it is important to study the issue of information security in distance learning. But first let's analyze the term "security."[2]

Security is the condition of protection from threats; it reflects imaginary substance of security and is the form of a subject's emotions. Security is not the state of protecting one's interests. Security in its wide sense is not somebody's state. It is the conditions of someone's existence under his or her control. As a result, we may conclude that security of distance learning includes not only security of soft- and hardware but also control of all the basic learning process functions. Besides, it is necessary to take into account that international educational programs are more vulnerable. Here is an example. A national (regional) university has an opportunity to control statistics of a distance course attendance in a form of its learners' IP-addresses, etc. It is difficult to provide a permanent monitoring and system configuring in case of international collaboration as this system should posses two contradictory features – it should be available for students from every point and should be protected from any threat from anywhere. The solution of this task lays in the control of the whole life cycle of the distance course, not only creation but also the stages of its usage.

To introduce a new form of knowledge acquisition, one should take into account that methods of education, content preparation and a lesson conducting style significantly differ from other methods used in educational institutions. The main problem of all universities is a lack of skillful and specialized staff. It is usually assumed that the author of a course is able to transfer it into the appropriate electronic format, to maintain and support a learning process as well. The practice turned out not to be so easy. In case of international collaboration, the situation becomes even more complicated. It is necessary for the tutor to be free of any national, cultural, or religious prejudices. It is absolutely prohibited to propagate knowledge that is not envisaged in curriculum and lesson plans. The ethical issues as well as special knowledge and skills are subject of some special courses to train tutors, to facilitate their acquaintance with some peculiarities of different nations and ethnic etiquette. A qualified tutor is characterized by the following basic features [3]:

1. Openness to consideration of a new problem;
2. Skillfulness to evaluate scalability and actualization of a problem aiming at discussing the issues that are most interesting for most of the participants;
3. Ability to choose the most accessible and secure way of communication depending upon the character of the problem and its solution;

4. Informing the participants in a dialogue about prehistory of the problem and its current state. Stating a clear and objective form of the problem free from individual subjective attitude;
5. Ability to work with an adult audience whose participants are well educated but not ready psychologically to change their social role to that of pupils.

There are different norms and scientific, economic and legal rights for electronic publications in different countries. It is very important to consider intellectual property rights; otherwise these scientific publications may appear to be unprotected on the territory of other countries. As a result, it is necessary to take into account all the legislative specifics of the countries where distance learning will take place. Besides, respective legal bases should be worked out in the countries where the course will be used, and till that time geographical spreading of distance learning has to be limited. Thus, activities aimed at security of distance education, including protection of the author's rights and ensuring that a certificate obtained through distance learning will be recognized in the students' countries should be planned.

As a rule, a distance course is considered to be open. However, only that part of it that is necessary for the tutor and user's work must be open.[4] Thus, the problem is determined by security of distance learning software and hardware. It is known that content that is conveyed to the learner may be presented in three forms as data, information and knowledge.[5] Data is fixed information about objects and phenomena. Information is processed data in a suitable form for decision-making and analytical research. Knowledge is processed information used for problem solving and decisions making, as well as "meta"-information about ways of processing and transformation of information for making decisions. Security of data is mostly a technological problem, security of knowledge along with the technological aspect has a strong economic constituent, while information security includes both of them. Such dualism of information is explained by its ability to be either public goods or commercial product depending on its content. Knowledge is a final product and always can be evaluated in economic terms no matter if it is a concrete, conceptual or metaknowledge which is kept and performed in various forms.

As a result, it is necessary to single out technological (data, equipment, communication channels), semantic (information security from purposeful distortion) and economic aspects of information security. Figure 1 presents general framework of analyzing security issues of distance learning.

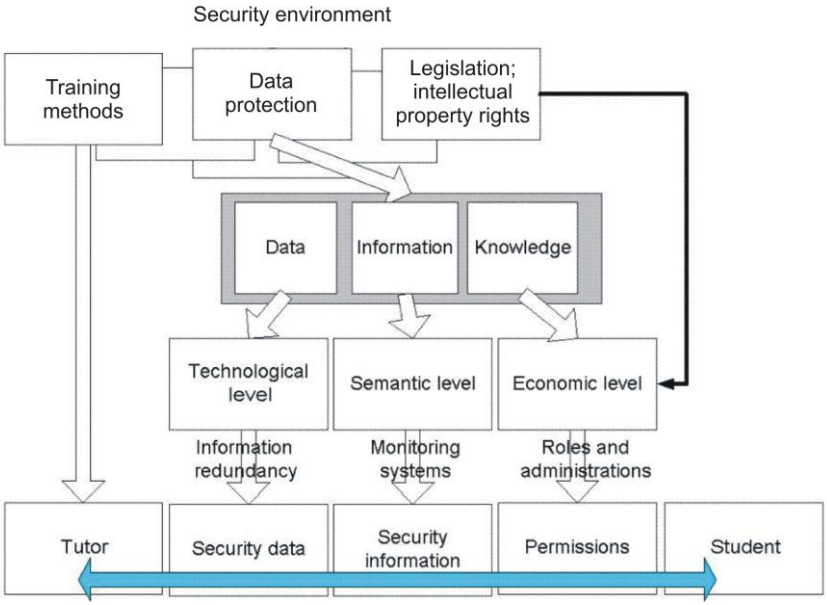

Figure 1: Monitoring tutor and student interaction by a security system.

Traditional methods to increase physical security of programs and data are based on information superfluity. Moreover, recovery and reservation methods are invariant to the information technologies applied in the data processing systems and are based on usage of redundant files (copies, damps, logs, etc.). Besides, these methods of "copying and recovery" not only ignore data processing technology and do not change it but also do not use its peculiarities. One should also note, that even terms "copy," "damp," "differential file," "system log," etc., do not bear any functional specifics of the information that is stored.

For the solution of the specified problems it is possible to introduce essentially new technological redundancy.[6] Functional-technical redundancy is understood as introduction of additional elements in data processing technology providing increase of programs' and data security. This redundancy can be of two types: procedural and file one. Procedural redundancy is understood as embedding additional procedures which take into account the specificity of the design decisions on realization of automated information-managing systems functions and intended for data security increase in data processing technology. Thus, the structure of system's information processing does not undergo changes. File redundancy is understood as introduction

of modifications in the information base of a system basing on its particular data processing technology. File redundancy can be subdivided into external and internal. Internal redundancy assumes no introduction of additional files, but adding fields and logic records in already existing files.

Within the framework of the open systems concept there are several integrated control systems, such as HP OpenView, Solstice, SunNet Manager and Unicenter TNG which are based on the management model offered by the International Organization of Standardization (ISO).[7] The ISO standard 15408-99 "Estimation criteria for information technologies security" may serve as an example. We shall consider the base features of control systems:

1. Fast localization of malfunctions - granting the information on the response time of a distance course modules and subsystems for rapid revealing of bottlenecks.

2. Detailed analysis of transactions - timing of all transaction performance stages, monitoring movement of a learner's request from a browser up to a web-server and further to applications and databases servers. The received data is automatically analyzed for revealing subsystems that may cause problems. The distance course built up on similar managing systems allows to trace and register:

- Through time of the response;
- Time of inquiry transfer through the Internet;
- Time of a web-site's response;
- Time of a request transfer from a web-server to the application server;
- Time of the application server response;
- Time of the separate COM components response;
- Time of a request transfer from one component to another;
- Time of the databases server response;
- Successful, interrupted and unsuccessful transactions of various types.

3. Automatic detection and revealing of all the web-transactions using the HTTP-protocol, independently finding out all components which participate in their processing and providing monitoring without long adjustment and control at the level of separate components. Control systems allow for tracing the distance course work at a level of separate components independently from the components implementation language.

4. Data aggregation and decomposition. By default, the speed of transaction-performance is defined by averaging the measurements received during an interval set up by the user. Control systems allow for measuring and registering

separate transactions performance time that can be useful while testing applications, searching for malfunctions or testing the adjusted configuration.

Control systems assist in locating problems in such applications, e.g. for distance learning, quickly allowing to answer the question of what is wrong: logic of the application or elements of an IT-infrastructure (networks, computers, systems of an intermediate level, etc.). Therefore, it is necessary to create products to ensure security within the framework of the open systems concept. These products should carry out intelligent control of hardware-software platforms on which applied information-telecommunications systems function.[8] Thus, this approach rejects a rigid universal scale of security classes. Instead, it is a flexible approach to the security estimation by ranging independent requirements and introducing protection profiles, allowing to define a set of necessary and sufficient requirements for each type of information technology products in view of their application conditions.

So, what is gained from ensuring security of distance learning? The first answer is – security itself. But if we return to the definition of security introduced at the beginning of this paper, the answer will be different. As a result we will have control on the process of new knowledge acquisition, thus approaching the solution of the equivalence issue of distance and local learning. By definition, distance education is just a different form of obtaining education that differs mainly by its organizational features. However, some problems may arise when a former student tries to get employed. The majority of employers do not recognize diplomas of distance universities for the reason of the absence of the control on the training process. Thus, the security of distance learning can promote problems solution for the given form of the education and its wide use.

Notes:

1 Vladimir K. Moroz, *About UNESCO Cooperation in Information Technologies of SIC Members in Distance Learning Area*, in Russian, <www.dlnet.unesco.kz/dsdc.html> (10 Dec. 2003).

2 G.V. Ivashenko, "The Main Point of Security," Presented at the 4th Annual Conference of the PfP Consortium of Defense Academies and Security Studies Institutes (Moscow, June 2001), p. 64.

[3] O. Briskina, "Network Cooperation Modeling in Tutors Distance Learning Training," Paper presented at the *Information, Technology, Education* conference (St.-Petersburg, 2003), 45-46.

[4] A.D. Danilov, N.V. Ivanova, E.I Kultishev, V.M. Kosmachev, "Integration of Open Education to Information Society," Paper presented at the *Internet and Modern Society* Conference IST-IMS'2001, in Russian (St. Petersburg, 20-23 November 2001), <http://ims2001.nw.ru/cgi-bin/one_tezis.exe?ivent=4&lang=RUS&ID_TEZ=47> (8 May 2004).

[5] M.I. Lugachev, "Information Security: Semeiotic and Economic Aspects," Presented at the 4th Annual Conference of the PfP Consortium of Defense Academies and Security Studies Institutes (Moscow, June 2001), p. 6.

[6] A. Shelkov, "Increasing Data Safety in Automated Information-Operation Systems with Functionally-Technological Superfluity," <www.sbcinfo.ru/articles> (10 Dec. 2003), in Russian.

[7] See for example Mark Timofeevich Kobzar, *Standard ISO/IEC 15408-99 and Its Implementation for Assessing IT Security* (Moscow, Center for Information Security, 2002), <http://www.fostas.ru/library/Kobzar2_e3.rtf> (8 May 2004), in Russian; Gene Troy, *Introduction to the Common Criteria for IT Security /ISO 15408/* (US National Institute of Standards and Technology, March 1999), <http://cnscenter.future.co.kr/resource/crypto/evaluation/cc/japan-brief-990318.pdf> (8 May 2004).

[8] V.V. Korneev, A.I. Masalovich, E.V. Savel'eva, A.E. Shashaev, "Recognition Program Modules and Detection of Unauthorized Actions Using Neural Nets," *Information Technologies* 2, 10 (1997), in Russian; V.V. Korneev, S.V. Sajin, "Control System for Computers Functionality and Network on Basis of Using Neural Nets," *Neural Computers: Development and Application* 1 (2000), in Russian.

KONSTANTIN ARKHIPOV and **VASILIY OVODKOV** are employees of the Information Technologies Laboratory of the Joint Institute for Nuclear Research. The Lab's hardware base allows to run complex experiments in the field of program realization of distance course. This is the first teamwork of the authors. Separately, they have over 20 scientific publications on distance learning, in particular on ways to increase its efficiency and security.

For correspondence:

Konstantin Arkhipov; Leninskiy, Gagarina st., 16, 28; Tula region, Russia. *Phone*: +7-095-755-56-55 (+3428), +7-910-425-14-59. *E-mail*: k.arkhipov@mail.ru.

Vasiliy Ovodkov; Pontekorvo st., 18, 12; Dubna, Moscow Region, Russia. *Phone*: +7-096-21-3-14-88, +7-910-441-63-29. *E-mail*: ovodkovv@mail.ru.