

DISTANCE LEARNING SYSTEMS AND THEIR INFORMATION SECURITY

SERGII KAVUN

Candidate of science (Economics)

IVAN SORBAT

IRINA SORBAT

Kharkiv

As it is known (Daniel, 1996), the area of distance (electronic) education (DE) cannot spare without the mutual influence of all related sectors and aspects of the operation; however, this statement can be applied to other areas. In addition, the solution of many global problems of DE, which is currently experiencing a certain crisis, is directly linked to the development of distance learning systems (DLS), based on information and communication technologies.

Problem of DE were discussed in studies of various scientists. In their opinion, the implementation of DE into the process of training and retraining of specialists in the educational system of different countries is necessary due to several reasons: 1) Slow mutual integration and implementation of European and world standards in education and research activity with regard to the principles of the Bologna process. 2) Intensity of science development requires permanent improvement of the professional knowledge and skills of employees of different specialties. 3) Only technology is capable of providing timely corrective training content by high-speed update of knowledge in information-educational environment. 4) High economic efficiency of DE.

In addition, the relevance of this question is that the implementation of DLS with their innovative methods of education can facilitate the solution of major social problems in the following ways: 1) Implementation of the population's needs for educational services. 2) Satisfaction of the country's needs in quality of trained specialists. 3) Increase of social and professional mobility of students, their social activity, level of self-consciousness, expanding of their mental outlook. 4) Preservation and increase of knowledge, hu-

man and material potentials, accumulation of national higher education. 5) Development of unified education space within the country and the entire international community, which suggests the possibility to get education in any place of educational space.

Statistical information. In order to emphasize the relevance of research of DE, a number of indicators (educational, social and economic) are considered below. As it is known (Daniel, Kanwar and Uvalić-Trumbić, 2005), DLS are based on the following key resources: users and development of the means (channels) of access (*Figure 1*).

In terms of Internet penetration, the distribution of the regions is shown on *Figure 2*.

The presented results reflect the real (at 31 of March, 2011) state of education in the world and by region, which shows that education level partly depends on economic situation of the region, population and other factors, but its require additional research. This indicator is more objective, because it shows the proportion of the Internet use among the entire population of the region.

As for the equity participation of actors in DLS, the statistics provides (Kavun, 2011) the following data (*Figure 3*).

A presented (*Figure 3*) ratio distribution of distance learning students to their total number demonstrates the inverse proportional dependence on the level of education system in a country taking into account the population correction.

Economic indicators in DLS must not be equal for the student and tutor (Bosseler and Carbonneau, 2009), taking into account the presence of fixed and variable costs. These are mainly financial (Kavun, 2007) costs (*Table 1*).

Thus, DLS can be represented in the form (Karpenko, 2008) of the scheme taking into account the cyclical nature of the study (*Figure 4*).

Then, considering the security aspects (Ponomarenko and Kavun, 2008), that are directly relevant to DLS, it is necessary to identify major elements of them (or subsystems-services), which the student would face with (*Figure 5*).

The research, which was conducted by the Center of Public Opinion Research NORC at the University of Chicago 10 years after the tragic event of 11 of September, 2001

showed the depressing result. It should be noted that Americans trust the information about different aspects of their private life only to governmental entities. *Figure 6* demonstrates students' attitudes towards the Internet.

Authors performed the analysis possible to implement decomposition of the learning process cycle (*Figure 7*).

Based on the author's analysis (*Figure 7*) of the educational process in the DLS, we found these main threats:

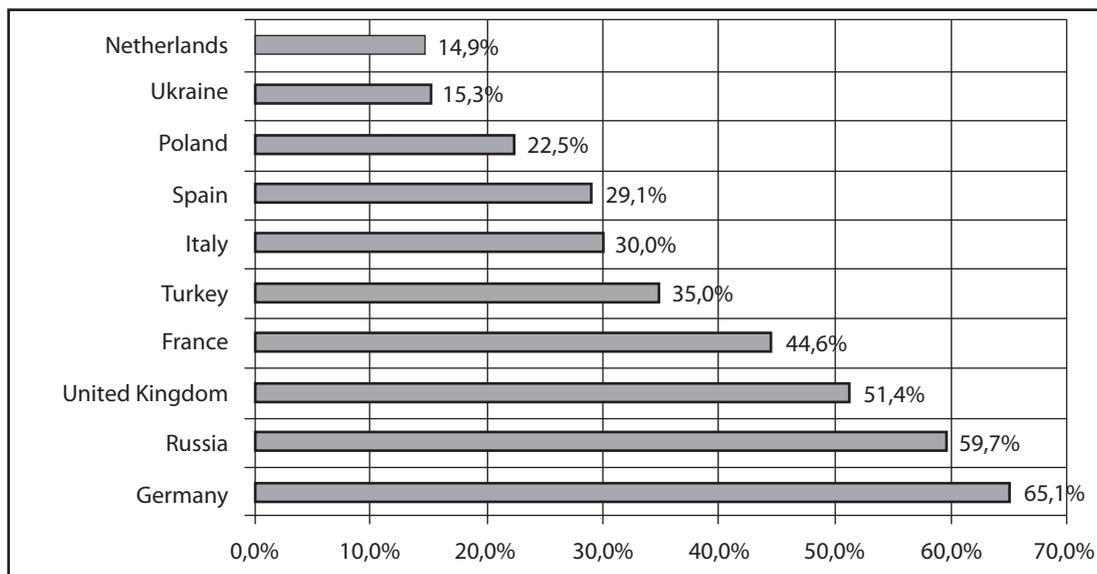


Figure 1. Number of Internet users in Europe (Source: Internet World Stats – www.internetworldstats.com): common indicator

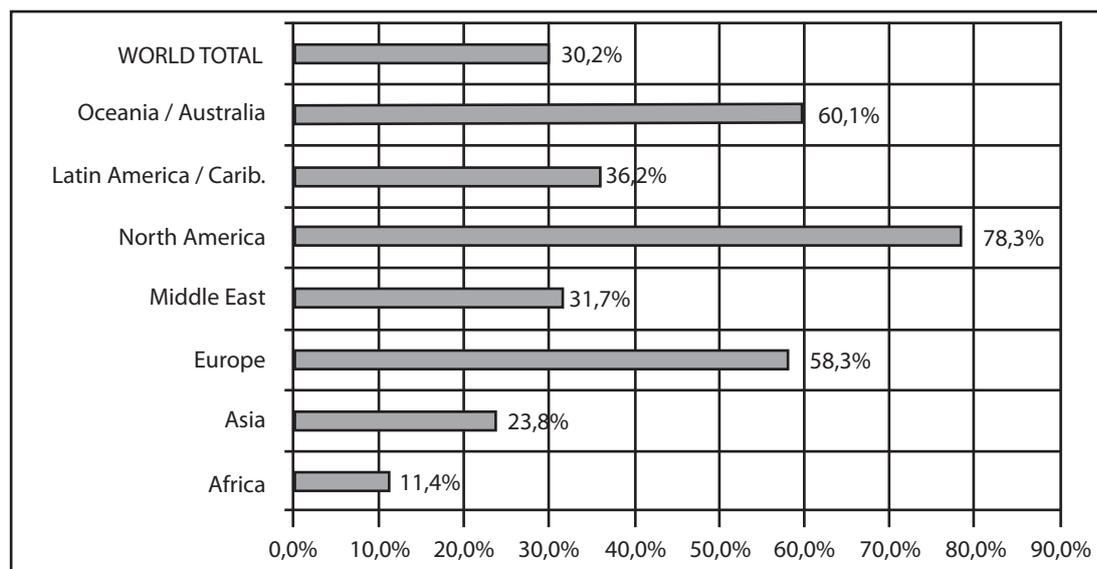


Figure 2. Word Internet Penetration Rates by Geographic's Regions – 2011 (Source: Internet World Stats – <http://www.internetworldstats.com/stats.htm>): common indicator

The importance of the Internet connection is only one of many discoveries of the Cisco last annual report, which were conducted in May – June 2011. There were a lot of respondents from 14 countries took part in the series of interviews including USA, Canada, Mexico, Brazil, The Great Britain, France, Spain, Germany, Italy, Russian Federation, India, China, Japan and Australia.

More statistics concerning this learning area is presented at the author's website (Kavun, Sorbat, 2011) [9].

Aspects of information security. DL is based on the use of traditional and innovative teaching methods and tools that are based on information and telecommunication technologies and provide an interactive learning process participants interaction and obtain, study and control of learning.

disclosure, integrity and denial of service. Additions were formed from characteristics and examples of possible attacks that can be implemented. ISS is part of the overall management system, based on risk analysis and is intended for the design, implementation, monitoring, and maintenance and improvement action in the field of information security (Ponomarenko and Kavun, 2008).

Examples of such countermeasures are also designed to be the authors (*Table 2*).

The authors describe a generalized scheme of constructing the ISS-model (*Figure 8*) that meets international standards.

In order to take into consideration all possible aspects of information security, we should highlight the key elements that influence the development of the DLS.

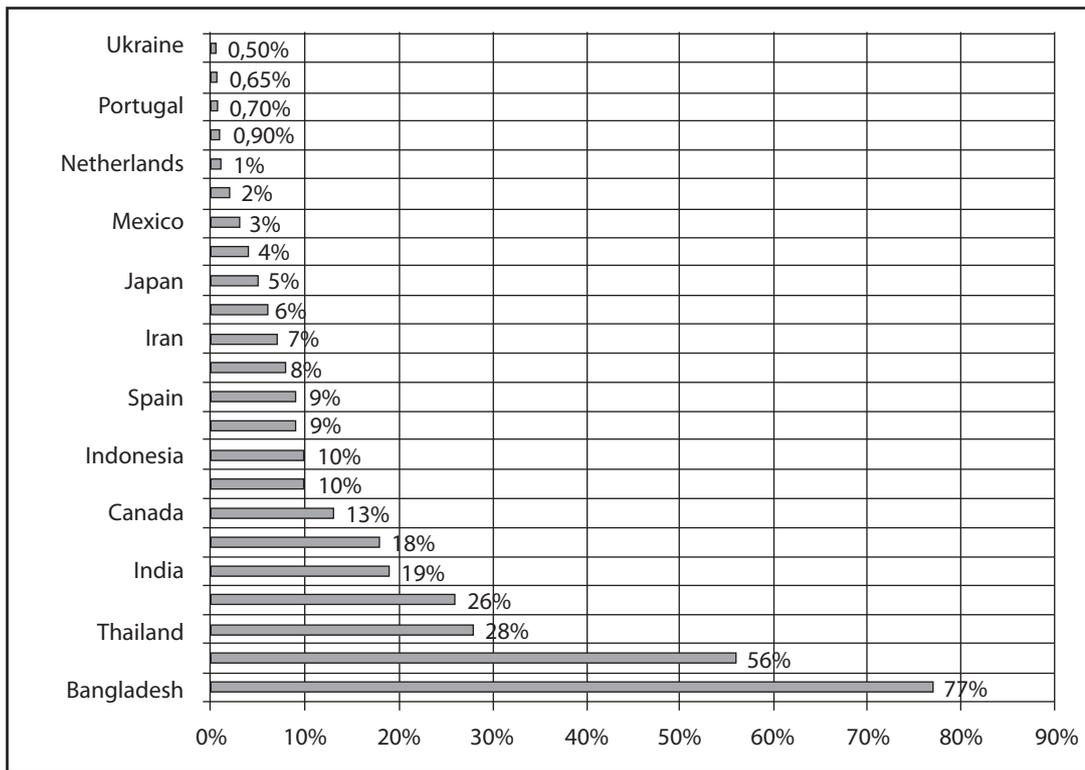


Figure 3. Proportion of students who study at distance from the total number of students: education indicator

Table 1

Types of expenses in the system of distance education: economical indicator (The result of author's researches)

| | Fixed expenses | Variable expenses |
|---------|---|--|
| Tutor | Elaboration of distance learning course | Support for hosting |
| | Elaboration of multimedia didactical ensuring | Allocation of personal time to participate |
| | | Testing |
| | Validation control works | |
| Student | The choice of course of study | Allocation of time for passing examinations |
| | Payment of course fees | Commissioning tests, exams |
| | The choice of learning mode | Payment of interim costs (printing, copying, subscription) |

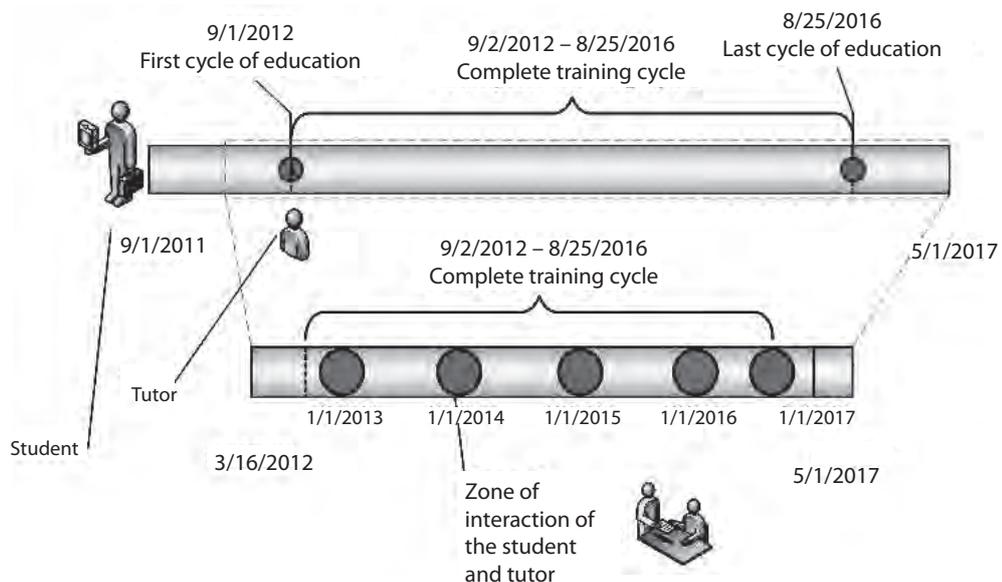


Figure 4. Cyclic scheme of the learning process over time (The result of author's researches)

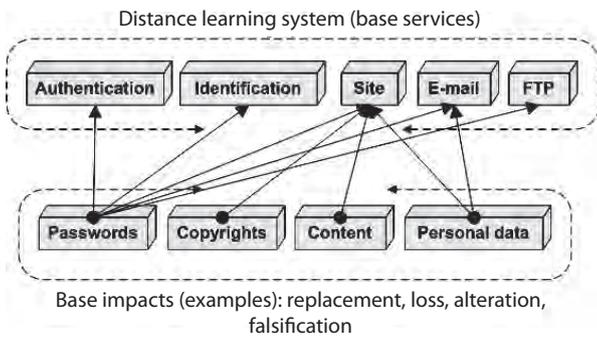
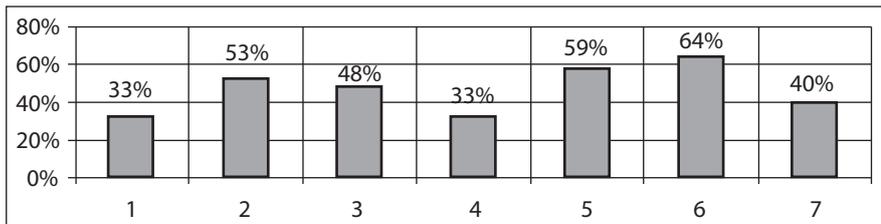


Figure 5. Influence of security factors on the DLS (Kavun, 2009)



1 – consider the Internet to be as important as air, water, food, and shelter; 2 – could not live without the Internet and cite it as an «integral part» of their lives; 3 – consider the Internet to be «close» in importance to water, food, air, and shelter in their lives; 4 – consider the Internet to be as important as these critical needs; 5 – indicate they could not live without the Internet, it is an integral part of their daily life; 6 – would prefer to have access to the Internet versus a car; 7 – consider the Internet to be most important in their daily life.

Figure 6. Results of the poll 1,441 College Students (aged 18 – 24) and 1,412 Employees (21 – 29) that completed an online survey (according to Cisco, May – June 2011)

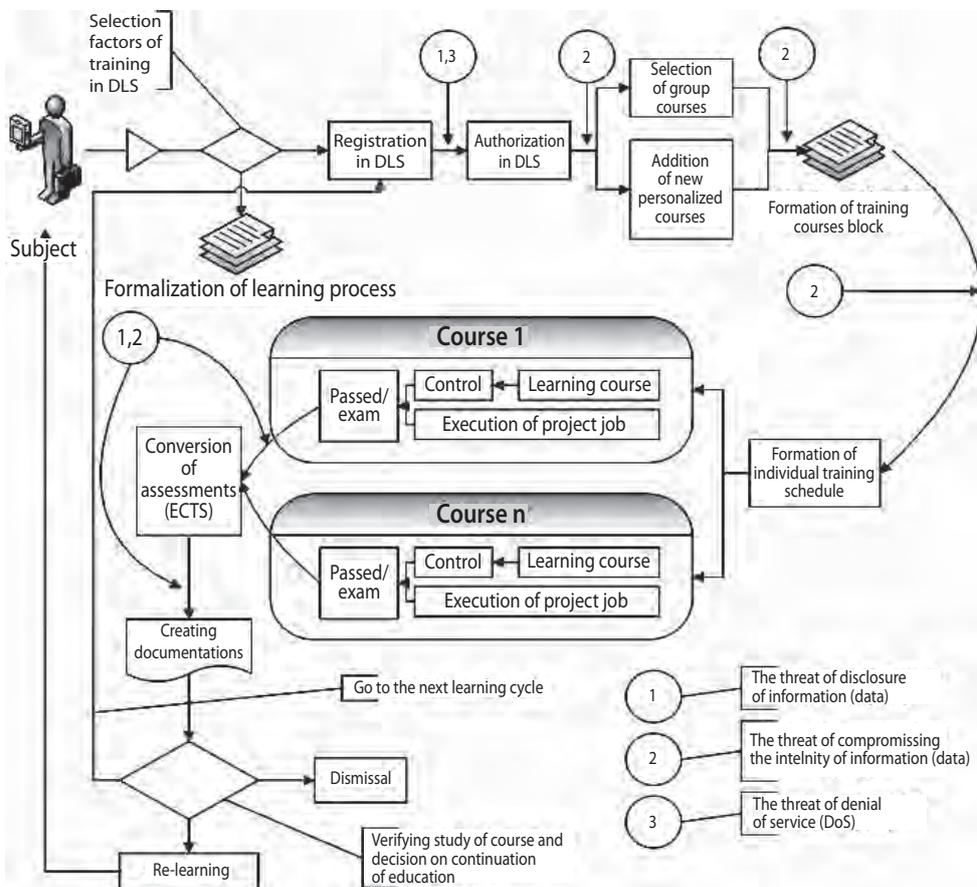


Figure 7. The scheme of the cycle of educational process in the DLS

What is the financial side of safety? For example, we present a few numbers that characterize this side. Hacking website or forum costs only \$ 50 (at a cost to build \$ 300 – 5000). The question immediately arises, «Is it worth then to spend money on creating a website?». The cost of a single account – \$ 20 – 25 (considering the total amount of \$ 80 million per year, it's the market earning crackers). Spam mailing costs from 50 up to \$ 200, depending on the volume of distribution. But this is the cheapest way of public relations, advertising, which can lead to the collapse of a marketing plan for the enterprises or other organizations. Breaking the mailbox costs from 15 to \$ 50, and this can be everyone's mailbox. At the same time other statistics show

that about 45% of the information in the category of trade secret is transmitted by e-mail (Kavun, 2011). To prevent these threats of unauthorized access, which is defined as access to information that is in violation of established rules of access permissions in the automated system, a necessary condition for a modification of DLS aiming at the improvement the level of information security (Kavun, 2007). Such improvement is possible when using the ISS.

Recommendations for countermeasures protect against unauthorized access

| Type of protection | Title of countermeasure | Description of methods and technologies of countermeasures |
|---|---|---|
| Protection from listening to a computer network | Detect listening | One of the major methods of listening detection is to use network intrusion detection programs, such as Network Flight Recorder (NFR). To protect at the level of individual nodes, you can use BlackICE from Network ICE, which allows it to discover ICMP-and TCP-listening, but also solve many other problems |
| | Prevention of listening | Necessary to evaluate the importance for DLS of data exchange on the ICMP-protocol between network nodes and the Internet. There are many different types of ICMP-messages, but in most cases there is no need to allow exchange of data using all available message types, so you need to block those types of messages that are not needed for work in the DLS. In addition, ACLs can allow the exchange of messages on the ICMP-protocol only with some well-known IP-addresses. Also one of the means of protection is the prohibition of unrestricted access to the ICMP protocol in the internal network, which helps to prevent DoS-attack |
| | Protection from IOMP-queries | Another method of protection is blocking IOMP-queries to those types that promote beyond publication of information about the network. At the border router to block passage in the internal network packets TIMESTAMP (ICMP-message type 13) and ADDRESS MASK |
| Protection from threats disclosing | confidentiality | The protection against threats to confidentiality of information should be provided in DLS cryptographic protection of data on hard and removable drives by their «transparent» encryption. For data encryption can be applied proven resistant encryption algorithms provided by: kernel-mode cryptographic driver that is part of Microsoft Windows (TripleDES algorithm with key length 168 bits) and connects an external package of additional encryption algorithms (AES with a key length of 128 and 256 bits, Twofish with 256 bit key length). In DLS should be performed regular re-encryption of protected discs with the change key and / or encryption algorithm. Necessary to provide cryptographic protection of network traffic management session, which eliminates its exposure or substitution of an attacker. Each protected disk can be determined by the individual scripts. These scripts can be used before connecting the drive, after connecting, before disconnecting, after disconnecting |
| Protection from threats integrity and denial of service | Ensuring the integrity and availability of data | To ensure availability and data integrity such technology is uses: expansion of drives during their filling. Secure drives can be created on the basic volumes of dynamic hard drives; individual scripts for each protected disk, support for multiprocessor systems and Hyper-Threading technology; stop of the process of encryption, decryption, or re-encryption should not lead to data loss, network traffic management session must be cryptographically protected, DLS must be organized by a group of administration to reduce the risk of data availability |

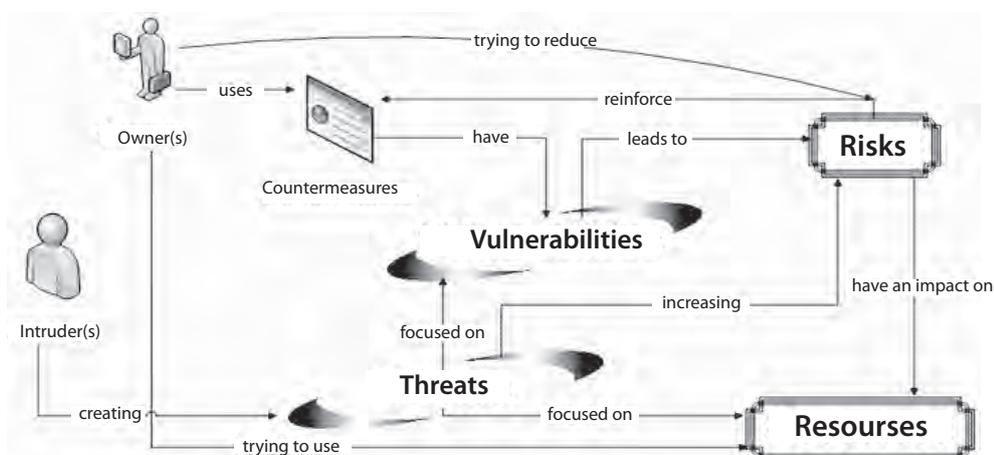


Figure 8. The common scheme to building of ISS-model

The use of watermarking technology in conjunction with the micro text will uniquely identify the authorship of content, therefore, will help to protect copyrights. Tools of WEB-validation confirm the stability of the code, the absence of malicious content, which ultimately leads to an increase of the credibility of the submitted materials, increases the rating and increases revenue. Authorization prevents from third-party developers claim or simply swindlers on the authorship, sue. Technology CAPTCHA (e.g., graphic interpretation) eliminates the effects of but autodialers, thus ensuring the objectivity of the statistics show, the audience and increase the degree of confidence. A reasonable hosting involves correct and optimal choice of provider (host) and provides the complex of the resources and technologies, which lead to an increase of population density, increase of functionality, increase of obtaining and providing opportunities.

Conclusions. Thus, the introduction and use of the above key elements will be deleted and if not protected, and then at least significantly reduce the impact of the consequences of negative impacts in the areas of information security:

1. Receive (or adjust) the value of content (such as for resale, we can give you an example from the Facebook): the copyrighting is widely developed nowadays. It all cause significant damage to the owners of educational resources, although most of the material have a public access.

2. Protect their copyrights (intellectual) rights: also it is a difficult question, which requires deep knowledge of international legal rights and results of litigation of violations and what is the most important, compensation for violation in copyrighting protection.

3. Can enter the world market (the same example with Facebook): such an achievement will have a positive influence on the company image, profit and rating; extend sphere of influence in their territory of activity.

4. Increase the ratings of educational institutions (due to the implementation of instructions of Ukrainian President to join the world rankings): for university to be in the rating (at the high position) has always a positive influence on the rating and the image of the university, providing the increasing of applicants number (due to the bigger importance and prestige), raising the status as a participant of different project, increasing the degree of belief and recognition of domestic and foreign universities.

5. Protect personal data and to ensure existing regulations: current state of users' personal data protection or other subject of educational activity entities requires providing a sufficient attention, the necessary funds and resources for preventing their leak (substitution, unauthorized access or other negative impact). Otherwise university takes a risk of significantly reducing their image or rate or to stop the existence.

6. Jointly raise the level of e-learning: as a result of the introduction and use of the above recommendations will increase the level of e-learning, put this form of training together with other forms to the appropriate location, and provide further practical use.

7. Establish a system of (complex) multimedia teaching systems, which will compete in the global market: the use of such system is a requirement of the modern world; because the technological development makes to implement various multimedia technologies to help the learning

process goes to a new, higher level. In addition, they make possible the increasing of distance education level if general, to facilitate its use and, thus, attract more participants into the education process.

Thus, distance education, which becomes obvious reality in the modern world and in the near future will develop most rapidly, because only through economic and technological advantages of this model can be satisfied with a huge demand for higher education, expected in developing countries. The optimal way of this development is creation of DLS, which based on information and communication technologies (Romanenko, Stolbov and Kalachova, 2009), with a guarantee of qualifying education, effective student support and an appropriate level of information security, which can be achieved by integrating the ISS into DLS. ■

REFERENCES

- Daniel, John S.** (1996). *Mega-universities and Knowledge Media. Technology Strategies for Higher Education*, London.
- Tabor, Sharon W.** (2007). *Narrowing the Distance: Implementing a Hybrid Learning Model. Quarterly Review of Distance Education (IAP)*, 8(1), 48 – 49.
- Casey, Anne M., Lorenzen, M.** (2010). *Untapped Potential: Seeking Library Donors Among Alumni of Distance Learning Programs. Journal of Library Administration*, 50(5), 515 – 529.
- Dickey, M.** (2005). *Three-dimensional virtual worlds and distance learning, British Journal of Educational Technology*, 36(3), 439 – 451.
- Moore, Michael G., Kearsley, G.** (2005). *Distance Education: A Systems View (Second ed.)*, Belmont, CA: Wadsworth.
- Daniel, J. S., Kanwar, A., Uvalić-Trumbić, S.** (2005). *Who's Afraid of Cross-border Higher Education? A Developing World Perspective, Higher Education Digest*, London, 52, 1 – 8.
- UNESCO Institute for Statistics.** (2006). *The World Education Report 2006. Comparison of World Education Statistics*, Montreal. URL (last checked 15 October 2011) <http://stats.uis.unesco.org/unesco/tableViewer/tableView.aspx?ReportId=175>
- S. Kavun.** (2011). *Statistical analysis in area of economic and information security.* URL (last checked 15 October 2011) <http://www.infeco.net>
- Kavun, S.** (2007). *Information security in business (in Russian).* Kharkiv national university of economics, Kharkiv.
- Ponomarenko V., Kavun, S.** (2008). *Conceptual Foundations of Economic Security (in Ukrainian).* Kharkiv national university of economics, Kharkiv.
- Kavun, S.** (2009). *System of Economic Security: methodological and conceptual positions (in Ukrainian).* Kharkiv national university of economics, Kharkiv.
- Kavun, S.** (2011). *Aspects of information and economic security in a system of distance education.* URL (last checked 15 October 2011) <http://infeco.net/infeco-overview/article/154-2011-05-17-05-27-57.html>
- Romanenko, I., Stolbov, V., Kalachova, V.** (2009). *The way of organization of knowledge control in Distance Learning Systems. The progressive information technology*, 2, 127 – 130.