Distance Learning Systems and their information security

Sergii Kavun[1]; Ivan Sorbat[2]; Irina Sorbat[3]
[1]*Department of computer systems and technologies, Kharkiv National University of Economics, Kharkiv, Ukraine*
[2] *Department of information systems, Kharkiv National University of Economics, Kharkiv, Ukraine*
[3]*Department of finances, Kharkiv National University of Economics, Kharkiv, Ukraine*
E-mail: *cc@ksue.edu.ua*

The article studies the problems of improving the degree of information security in the distance learning systems (DLS) at the expense of using innovative methods and technologies of information security systems (ISS). In this article are also considered the recommendations for improving existing DLS in training of the specialists at higher educational institutions as per Bologna Process regulations. In addition, this article demonstrates the results of statistical researches in the field of information security for DLS. The types of expenses in the DLS are also classified here. The authors have proposed the key elements for the DLS, the use of which is shown in the example of a research portal of information security. The arguments presented will increase the level of security. The results of analysis, carried out within this article, demonstrate the real possibility of development and further implementation of security elements. The results of analysis, carried out within this article, demonstrate the real possibility of development and further implementation of security elements.

Keywords: Distance Learning Systems, DLS, Security, Safety, Distance Education, Information Security Systems

Introduction

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. The traditional system of DE with its restricted access to universities, with relatively high cost and inflexibility is unable to cope with growing demand for higher education and unable to provide equal access to education for the general population.

What is DLS? Distance education (DE) or distance learning (DL) is a field of education that focuses on teaching methods and technology with the purpose of delivering teaching, often on an individual basis, to students who are not physically present in a traditional educational setting such as classroom. It is described as "a process of creating and providing access to learning when the source of information and the learners are separated by time and distance, or both" (Honeyman and Miller, 1991). Distance education courses that require physical on-site presence for any reason (including taking examinations), are considered as hybrid (Tabor, 2007) or blended courses of study.

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:

- Slow mutual integration and implementation of European and world standards in education and research activity with regard to the principles of the Bologna process.
- Intensity of science development requires permanent improvement of the professional knowledge and skills of employees of different specialties.
- Only technology is capable of providing timely corrective training content by high-speed update of knowledge in information-educational environment.
- High economic efficiency of DE.

Issues associated with theoretical and practical aspects of implementation of distance learning technologies which are deployed in modern education, are discussed in the works (Casey and Lorenzen, 2010; Dickey, 2005). Modern technologies and methods of teaching, learning and knowledge control are comprehensively considered in the works (Levinson, Moore and Kearsley, 2005).

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:

- Implementation of the population's needs for educational services.
- Satisfaction of the country's needs in quality of trained specialists.
- Increase of social and professional mobility of students, their social activity, level of self-consciousness, expanding of their mental outlook.
- Preservation and increase of knowledge, human and material potentials, accumulation of national higher education.
- 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).

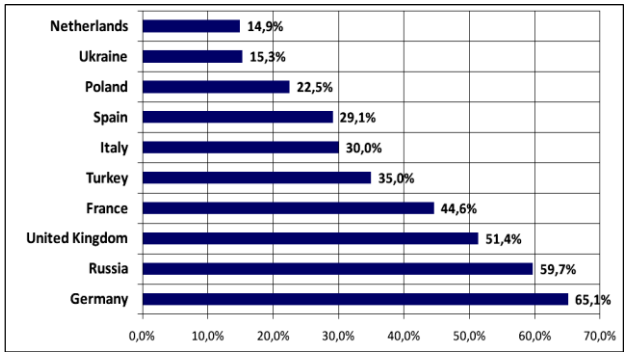


Figure 1.
Number of Internet users in Europe (Source: Internet Word Stats – www.internetworldstats.com): common indicator.

For example, as it is shown, Ukraine was on the 9th place among the countries of Euro-region with the index of population of 33.9%, i.e. at least every third person here knows what the Internet is and can use it.

According to the result at Figure 1 it is possible to make an inference that presented distribution completely corresponds to the share of users (at 30 of July, 2011) in Europe. It based on population of each country from which this distribution has a direct relationship.

Thus the level of growth of this knowledge in Ukraine is over 7500% per year (UNESCO Institute for Statistics, 2006).

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

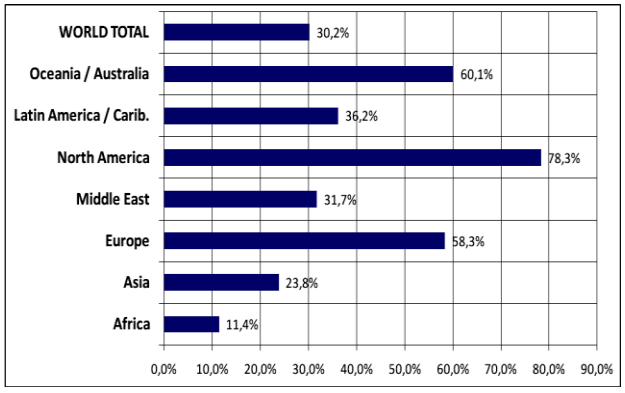


Figure 2.
Word Internet Penetration Rates by Geographic's Regions – 2011 (Source: Internet Word Stats – http://www.internetworldstats.com/ stats.htm): common indicator.

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.

Obtained statistical data can be used to conduct a comprehensive analysis of the structure of existing DLS, detection of vulnerabilities in them and threats of unauthorized access, implemented through the existing vulnerabilities, for proposing a model of the information security system, and formulation of conceptual recommendations for modifications (improvements) of DLS.

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

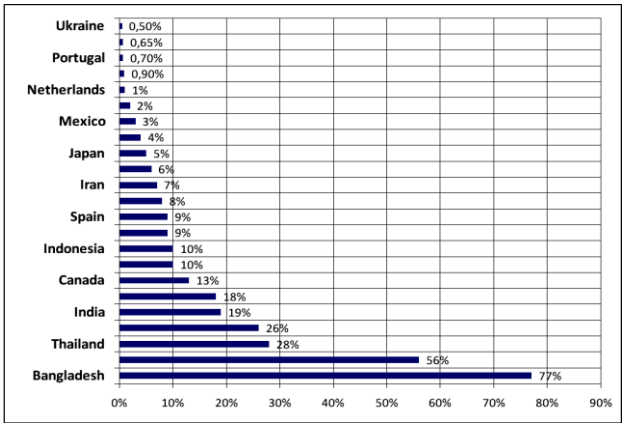


Figure 3.
Proportion of students who study at distance from the total number of students: education indicator.

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.

For example, in Canada (UNESCO Institute for Statistics, 2006), every tenth student has direct relevance to the DLS. This indicator provides Canada with the fourth place among countries of the world. As we remember, at the accounting classification there are 191 countries-members of the United Nations, and the total number of countries is more than 240.

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).

Table 1.
Types of expenses in the system of distance education: economical indicator (The result of author's researches).

	Fixed expenses	Variable expenses
u t o	Elaboration of distance	Support for hosting

	learning course	
	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)

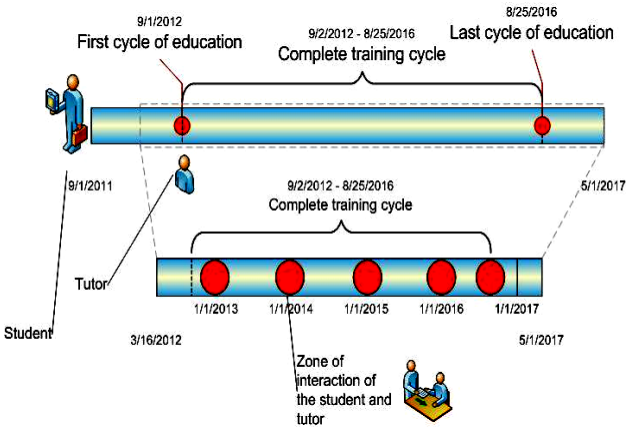


Figure 4.
Cyclic scheme of the learning process over time (The result of author's researches).

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).

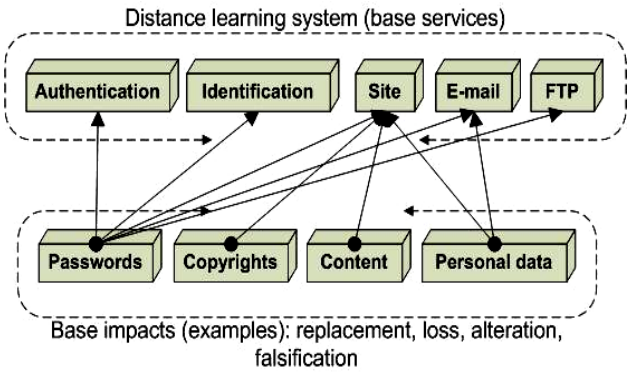
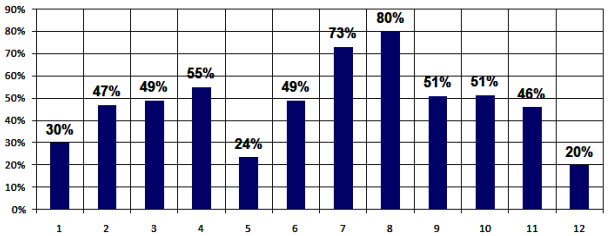


Figure 5.
Influence of security factors on the DLS (Kavun, 2009).

They are based on items considered by student representatives. The results of the survey of university students in Chicago are demonstrated on Figure 6.



1- positive attitude towards the government to read personal mail without permission; 2 - positive attitude to reading the data when it is necessary to communicate with foreigners;3 – thinking, that government must be able to browse someone's search history without judicial authorization; 4 - financial records can also be inspected without proper notice; 5 - positive attitude towards the government's listening to personal phone calls; 6 - positive attitude towards the government's listening to personal phone if calls are directed abroad; 7 – approval of video surveillance in public places; 8 – approval of video surveillance in public places, if respondents have children; 9 – consideration a torture of people, suspected of terrorism, to be a norm; 10 – approval of "harsh interrogation measures" on people, suspected of terrorism; 11 – consideration a torture to be illegal; 12 – thinking, that U.S. is now on the right way

Figure. 6.
Results of polling of U.S. citizens at the University of Chicago (according to NORC, September 2011).

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.

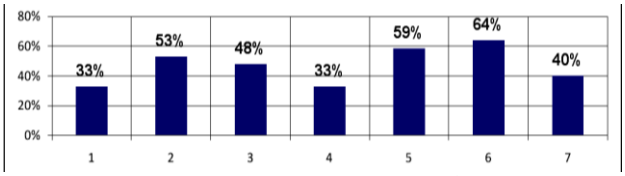
Gathering of such information by private companies evokes protest from USA citizens; - it will be enough to remember precedents with mobile devices running by iOS and Windows Phone.

Owners of these devices expressed their protest and it led to legal action.

Nevertheless, in the Register edition was written that only one in five respondents believe that USA now is moving in the right direction.

Among the factors considered a special place is occupied by the following ones: authentication, identity, website and communication tools (FTP-and e-mail-services) (National initiative for cyber security education, 2011). All of them in aggregate or individually promote the use of passwords, personal information, content, and copyright compliance. At the same time in the past these factors were subjected by negative impact from substitution, loss, alteration, falsification and other negative aspects of information security (Hoover, 2010). Figure 7 demonstrates students' attitudes towards the Internet.

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.



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 7.
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).

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

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.

Authors performed the analysis possible to implement decomposition of the learning process cycle (Figure 8).

For the traditional education system common sources of learning are only printed materials, while innovative education

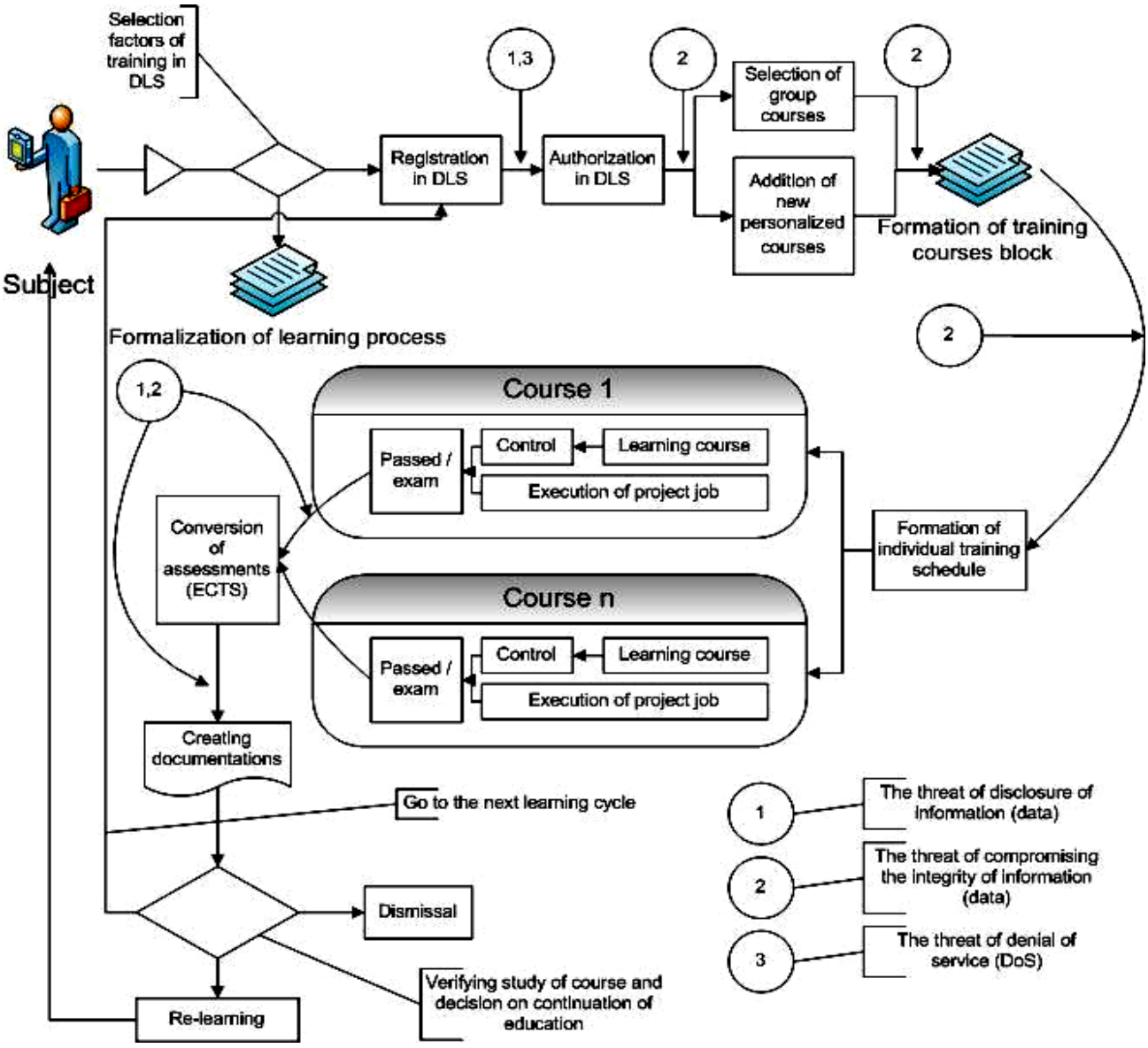


Figure 8.
The scheme of the cycle of educational process in the DLS.

involves the use of both printed and audio-visual materials, computer teaching programs, electronic journals, online databases, and other educational materials provided to the listener through computer networks. Therefore, this study raises the problem of prediction of organizational and technical means of safe and confidential storage, usage and transfer of data through these networks.

Based on the author's analysis (Figure 8) of the educational process in the DLS, we found these main threats: disclosure, integrity and denial of service. Additions were formed from characteristics and examples of possible attacks that can be implemented (Table 2).

Table 2.
Types of expenses in the system of distance education: economical indicator.

Main threats	Characteristics	Vulnerability	Examples of possible attacks
Disclosure	This threat shows that the information may be known to those who shouldn't know. Threats of disclosure take place whenever the access to certain confidential information (e.g. personal data) is received.	Threats of disclosure become possible at the stage of authorization and generate documentation	At the stage of authorization attacker can intercept the authentication data, while at the stage of creating documentation – can remove confidential information about success of student training
Integrity	This type of threat includes any deliberate change (modification or even removal of data)	Threats to integrity occur on stages of receipt of regulatory and variable blocks of courses, the formation of such courses, as well as converting assessments and creation of the documentation	Any substitution or modification of data on success training can lead to consequences that are described in (Kavun, 2011)
Denial of service (DoS)	Threats of denial of service occur when the actions of the attacker block the access to certain resource of DLS	This type of threat can be realized on the stage of logging in DLS	The implementation type of threat "denial of service" at the stage of logging in the DLS, can lead to disruption of lessons which take place in synchronous mode

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). The main purpose of any ISS is to ensure sustainable operation of the facility, prevention of threats to its security, protection from unlawful acts, to prevent disclosure, loss, leakage, modification and destruction service information, ensure the normal functioning of all departments of the object. Examples of such countermeasures are also designed to be the authors (Table 3).

Table 3.
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 JCMP-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.

The authors describe a generalized scheme of constructing the ISS-model (Figure 9) that meets international standards:

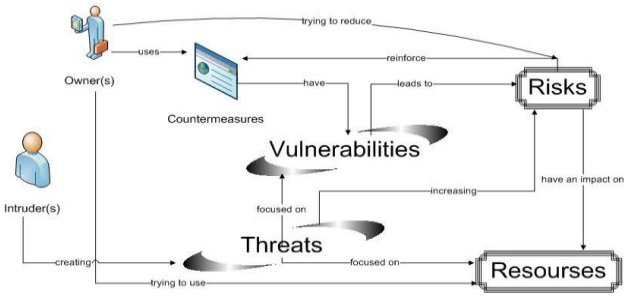


Figure 9.
The common scheme to building of ISS-model.

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.

All disputes or created by the negative aspects of information security (Rezgui, 2007) entail the emergence of aspects of information security, which together form the financial (monetary) loss. This is confirmed by the following numbers according to data 2010-2011: the numbers of stolen records of personal data – 3.9 million per year; increase in the number of incidents – 1.5-2 times per year; costs for the organization to support the information security – 127 hours per month; proportion of organizations having problems using the password – 90% (Kavun, 2011).

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.

ISO / IEC 15408 "Information technology – Security techniques – evaluation criteria of information security," and the ISO / IEC 17799 "Information security management", and takes into consideration trends in the regulatory framework for information security.

Therefore, because the DLS revealed several threats of unauthorized access, it should form and hold complex of means and measures (countermeasures) that would have eliminated all points of risk threats implementation.

Thus, the influence aspects of information security development on DLS become obvious.

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. In many countries for copyrighting no punishment or fine are provided for. Besides, it is very difficult to see and prove the commission of this act. 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. In this aspect knowledge of the information will significantly facilitate the possible consequences based on results of trials in copyright confirmation.
3. Can enter the world market (the same example with Facebook, if you remember how it all began): such an achievement will have a positive influence on the company image, profit and rating; extend sphere of influence in their territory of activity. Besides, entering the global market is a natural desire (and international recognition) of any enterprises, including educational institutions.
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), rais-

ing 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. Modern multimedia technologies allow to present material to study more clearly and simply and moreover they can make the process dynamic.

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.

Honeyman, M., Miller, G. (1991). Agriculture distance education: A valid alternative for higher education? Proceedings of the 20th Annual National Agricultural Education Research Meeting, December, 67–73.

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.
doi:10.1080/01930826.2010.48859

Dickey, M. (2005). Three-dimensional virtual worlds and distance learning, *British Journal of Educational Technology*, 36(3), 439–451.

Levinson, David L. (2005). Community colleges: a reference handbook, ABC-CLIO.

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

Bosseler, D., Carbonneau, D. (2009). E-Learning. The World Bank. URL (last checked 15 October 2011)
http://go.worldbank.org/PBR14X5FK0

Kavun, S. (2007). *Information security in business (in Russian)*. Kharkiv national university of economics, Kharkiv.

Karpenko, O. (2008). Distance education in word countries: scale factor. URL (last checked 15 October 2011)
http://www.old.muh.ru/.Docs/content/public/public_2008_karpenko_om.doc?user=6d3ee0981853e5affe47302bf793e7e5

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.

National initiative for cyber security education. (2011). DHS. National initiative for cyber security education. URL (last checked 15 October 2011)
http://csrc.nist.gov/nice/awareness.htm

Hoover, J.N. (2010). NIST tackles cyber security education. The National Institute of Standards and Technology will spearhead the national cyber security workforce development and awareness campaign. *InformationWeek*. URL (last checked 15 October 2011)
http://www.informationweek.com/story/showArticle.jhtml?articleID=224700519

Rezgui, Y. (2007). Information security awareness in higher education: An exploratory study. *Computers & Security*, Montreal, 27(7-8), 241-253.

Kavun, S. (2011). Aspects of information and economic security in a system of distance education. URL (last checked 15 October 2011)
http://infeco.net/en/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.