Analysis of Information Flows of Distance Education Systems, Taking into Account the Need to Ensure Their Cybersecurity

Valery Lakhno[1], Lazat Kydyralina[2], Berik Akhmetov[3], Bagdat Yagaliyeva[3], and Kayirbek Makulov[3]

[1] National University of Life and Environmental Sciences of Ukraine, 19 H. Rodimtseva str., Kyiv, 03041, Ukraine
[2] NJSC "Shakarim University in Semey," 163 Shugaev str., Semey, 070000, Kazakhstan
[3] Yessenov University, microdistrict 32, Aktau, 130000, Kazakhstan

Abstract

A structure for organizing information flows (IF) in distance learning systems (DLS) of universities is proposed, which is able to increase the efficiency of the complex interaction of both existing and new promising mechanisms for controlling and processing IF that circulate in DLS. The proposed additions imply the development of new or the use of ready-made models of protected information flows (IF) and DLS processes. And besides, the features of optimization measures related to the information security of the DLS are taken into account. The proposed model covers a set of conditions and tasks that are priority when searching for optimal information security measures for DLS.

Keywords

Distance learning system, information flows, cybersecurity, information security.

1. Introduction

In the context of the global digitalization of society, distance education systems (DLS) are becoming more and more widespread in the field of education, due to their inherent qualitative characteristics and features [1–4]. At the same time, the tasks of ensuring cybersecurity (KB) of information flows (IF), which contain confidential information and belong to the DLS, or are part of its workflow, were updated [5]. The existing standard solutions for CS od DLS, according to many researchers [6–8], are only able to partially solve problems related to IS and CS od DLS.

2. Analysis of Previous Studies

Many authors [1–8], dealing with the issues of providing IS and CS of enterprises in the digital sphere, and this can undoubtedly include the digital educational environment of the university (DEEU), have shown that the most effective approach can be the one in which the information flow management system (IF) inside the DEEU is made based on the separation of the goals of the functioning of these flows, as well as the content that each flow contains.

During the research, there was performed an analysis based on the results of an audit of IS and CS of international companies dealing with relevant issues for state organizations, including universities and other large educational institutions (EI). First of all, they are EU, the USA, and Canada [6]. As the results of such studies [7] showed, as well as the data cited in [5], and not taking into account specific targeted attacks aimed at buffer overflow and violation of cryptographic protocols [6], a significant number of violations is associated with unauthorized data changes in DEEU (> 12%), with bypassing the restrictions policy on IS in DEEU (> 15%), with insufficient protection of the authentication procedure, etc.

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: lva964@nubip.edu.ua (V. Lakhno); lazat_75@mail.ru (L. Kydyralina); berik.akhmetov@yu.edu.kz (B. Akhmetov); bagdat.yagaliyeva@yu.edu.kz (B. Yagaliyeva); kaiyrbek.makulov@yu.edu.kz (K. Makulov)
ORCID: 0000-0001-9695-4543 (V. Lakhno); 0000-0002-2836-0919 (L. Kydyralina); 0000-0003-2860-2188 (B. Akhmetov); 0000-0003-4644-2261 (B. Yagaliyeva); 0000-0002-0826-0371 (K. Makulov)

Different according to the source data [7] can be the targets, objects and subjects of cyber attacks on DEEU, see Table 1.

Table 1

Aims, objects and subjects of attacks on DEEU(according to [7])

Types of cyberattacks			
Cyber espionage is unauthorized transmission using hidden (undeclared) data communication channels, IP programs, etc.).	Cyberaudit is development of cyberattack scenarios, hacker and "friendly" cyberattacks, search for vulnerabilities in the DEEU.	Cyber fraud is the "sale" of fake electronic documents, and etc.	Cyber sabotage is a decrease in productivity, including at the expense of the DEEU resources, in particular, till a complete stop of the educational process.
Objects of cyberattacks			
Information Systems of EI.	Own or ordered software of EI.	EI databases,	Local network component.
The objects of cyberattacks on DEEU are: IS of EI, distance education systems, database servers, data of students, staff, support staff, etc.			
Attacking side			
Novice hackers, professional hackers, competitors, insiders, organized crime groups, etc. At the same time, the level of technical equipment and competence of the attacking side can be quite high.			

For several years, analysts in the field of IS and CS have fixed a trend indicating a steady increase of the number of cyber incidents and cyberattacks in DEEU.

This, in particular, can be explained by the increase of the number of local networks of universities and other EI that are connected to public networks [6].

In publications devoted to the problem of evaluating the security of DEEU [5] it is noted that in addition to the technical tasks on protection of the information circulating in ICSU, it is necessary to analyze periodically information risks and to monitor the effectiveness of the implemented measures aimed at ensuring IS and CS of the university. These procedures allow to consider:

- The variability of requirements in the tasks of information protection (for example, from content protection to protection of personal information of employees and students).
- The potential possibility for the emergence of new cyberthreats and vulnerabilities in ICSU.
- The decrease of the effectiveness of already implemented measures for information protection over time.
- The decrease of the reliability of information processing in IEEU by physical obsolescence of the equipment and software.

Thus, within the framework of this subsection of the research, we will consider the task of creating a DLS structure that would take into account the degree of security of individual information flows within the DEEU, and would also potentially be able to provide control over the IF, as well as protect the DLS from arbitrary information attacks by computer intruders.

For DLS, as for most digital systems, there are two types of key threats that, to one degree or another, can affect the level of students' preparation, as well as the performance of DLS as a whole. Such groups of threats, without a more detailed classification, to which a fairly large number of studies by other authors are devoted [9–15], include:

- External threats, i.e. remote influence on the DLS of an attacker, for example, aimed at creating opportunities for illegal penetration into the DLS.
- Internal threats, unlawful introduction by malefactors of foreign information flows into the DEEU, in particular, into information systems, using vulnerabilities and weaknesses in the DLS protection circuits.

We believe that in order to realize the main mission of the DLS, i.e. to give chances to all students, regardless of their location, economic social, and other conditions, to receive a quality education and at the same time remain cost-effective and competitive, any DLS of a modern university should have the following properties:

- Qualitatively and promptly process information flows that circulate in the DLS, as well as in the DEEU as a whole.
- Contribute to a continuous and stable cycle of work of the DLS.
- Ensure the confidentiality of personal data of teachers and students who use DLS.

Purpose of the study is development of models of protected information flows (IF) and processes in DLS, which will allow taking into account the features of optimization measures related to IS of DLS.

3. Models and Methods

Based on the above, it is possible to present the structure of the DLS and its main information flows, based not only on the functional requirements for the DLS, but also taking into account the need to solve the problem of ensuring information and cyber security of such systems. The block diagram is shown on Fig. 1. This approach allows, to the extent necessary, to take into account both the basic requirements for the DLS, and take into account the tasks of protecting information flows within the system.

In case of the emergence of external information flows, indicated in diagram 1 as "**1**", they must first be processed in the block responsible for collecting and processing information before getting into the DEEU and its DLS component (on Fig. 1. designated as BCPI). This block, in accordance with the recommendations [15–18], implements the following functions:

Analysis of incoming traffic and protection of DLS from external ones (cybersecurity block - CSB);

IF analysis (information flow analysis block - IFAB). This block is intended for: (a) IF monitoring - tracking IF circulating in the DLS, as well as their accounting and accumulation of statistics; (b) analysis of IF from the functional units of the university; (c) encoding-decoding IF, and the formation of specialized IF, which are intended exclusively for students; (d) IF routing; (e) protection against internal threats.

Planning (Planning Block, PLB). This block is designed to collect, store and backup information that circulates in the DLS).

Implementation (Implementation Block (IMB). This block is intended for the subsequent implementation of the plans and data developed in the IMB.

Each of the above functions can be implemented based on the work of their own algorithms to solve the tasks. The coordinated work of all blocks is able to filter out "potentially dangerous" or "malicious flows" (viruses, spam, etc.), which will prevent the implementation of many external and internal cyber threats for DLS.

Upon successful verification in the CSB, the IF-1 information flow is transmitted to the analysis unit, i.e. in AB. The block diagram of IFAB operation is shown on Fig. 2. As mentioned above, IFAB performs the work of evaluating and processing all information flows circulating in the DEEU and DLS, and most importantly, registers and analyzes the status of "encoded IF." If the current IF, located in the IFAB, does not pass the check for this status, the encoding procedure is performed in relation to it. By encoding, we mean the implementation of the procedure, when, based on the sets of goals and semantic elements, a new IF will be formed with a formalized structure that corresponds to the expression:

$$M_{C\,INFL} = \left[M_{ind}, M_{sem}, M_{con}\right], \quad (1)$$

where $M_{C\,INFL}$ is structure of the encoded IF; M_{ind} is a set of indices that determine the ownership of IF; M_{sem} is set of semantic IF content; M_{con} is a set of initial content corresponding to the IF.

Therefore, it is possible to implement protection against basic internal threats in the IF section "1-2". Of course, for this it is necessary, based on the architecture of a particular DLS, to select adequate means and methods of protection.

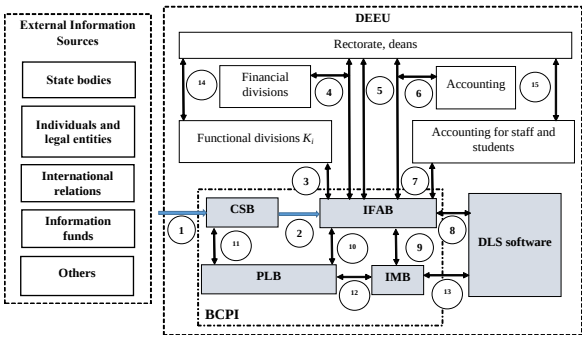

Figure 1: Scheme of DLS information flows, taking into account the need to ensure their cybersecurity

In order for a targeted or accidental malicious IF to be processed in the DLS, it must first be converted to the IF format accepted in the system. Otherwise, this thread will be ignored. At the same time, after encoding, the initial IF will lose its initial activity, and, therefore, will no longer pose a direct threat to the DLS.

If the IF meets all the requirements, primarily in terms of IS and CS, then based on the set M_{ind}, this IF will be forwarded to its recipients, based on the routing algorithm and tasks. These IFs on Fig. 2 are designated by the positions 3–10. We believe that the DLS works in conjunction with the electronic document management system (EDMS), which are now being widely introduced into the digital environment of universities around the world [1–4]. Such an organization of IF circulation in the DEEU and DLS will increase the efficiency of all structural units of universities that

are responsible for organizing distance education, primarily by updating a specific IF within the framework of only their own functional tasks.

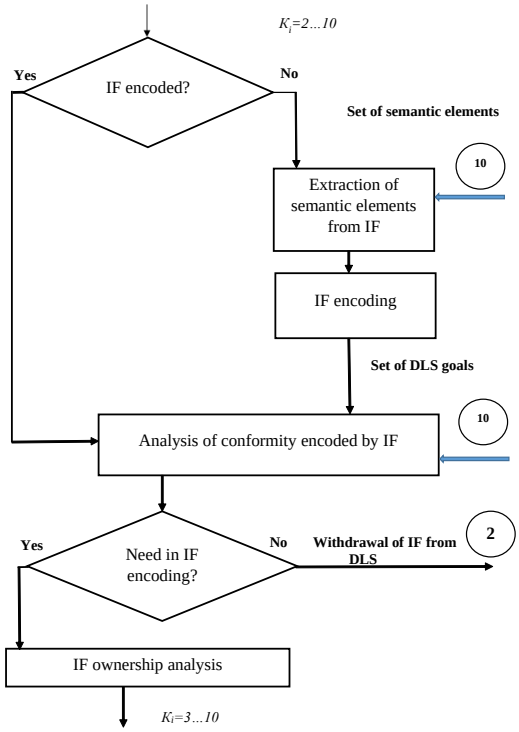

Figure 2: Block diagram of processing information flows in the analysis block

To maintain the relevance of the information arrays (IA) contained in the DLS and their backup copies, the PLB is used. This contributes to solving the problem of restoring IA and monitoring their integrity in cases of accidental failure or targeted destructive impacts on the DLS by computer intruders.

In case where the analyzed IF contains requests for the provision of a certain course or other educational content, control actions (CA) should be automatically generated in the IFAB, which are then sent to the CA. The result of the implementation of the CA will be the formation of a virtual environment that contains elements that contribute to the implementation of the request.

Based on the scheme of information flows of DLS, taking into account the need to ensure their cybersecurity, a fundamentally new methodology for creating an IS support system for DEEU and DLS is proposed. The methodology contains the following steps:

1. Determination of the probability of the impact of IS and CS threats on the DEEU and/or DLS.
2. Determination of a generalized indicator of the level of IS and CS of the DEEU and/or DLS.
3. Evaluating the effectiveness of investments in IS and CS of the DEEU and/or DLS.
4. Creation of an integrated mechanisms for providing IS and CS to the DEEU and/or DLS.

The proposed structure for organizing information flows in the DLS of universities, in our opinion, is able to effectively implement the complex interaction of both existing and new promising mechanisms for controlling and processing IF that circulate in the DEEU and DLS.

Cyber attacks on DLS [5, 6, 15, 17] lead to information loss, equipment and hardware failures, significant material and moral losses that are inflicted on the owner and users of the network and the DEEU as a whole. Most often, a cyber attack is a consequence of the presence of weaknesses in the DEEU, its information networks (InN) or in their protection systems. That is, a vulnerability is a weakness in the information assets of the DEEU or in the ISS, leading to the possibility of implementing certain cyber threats. Therefore, in order to counteract the main cyber threats, the information security system of the DLS should solve the following tasks:

- To delimit and control the access of subscribers (users) to the resources of the DLS or/and InN.
- To implement functions for the protection of data transmitted within the framework of the relevant information flows through communication channels.
- To register, collect, store, process and issue information about all events (including incoming and outgoing flows) that occur in the InN, DLS or DEEU.
- To implement monitoring of the work of users of InN (DLS).
- To ensure that the operating environment is closed for already tested software.
- To implement protection against uncontrolled introduction of potentially dangerous software into the InN (DLS) (for example, containing “bookmarks” or leading to critical errors).
- To carry out self-defense against means of overcoming the information security system and protection against the introduction and spread of malicious software.
- To ensure the availability of DLS information resources, for example, by data backup.

- To ensure and control the integrity of critical resources for the DLS or DEEU as a whole.

During the research, the method of managing the IS of DLS or DEEU was considered. The method is based on a set of optimization models, and the main steps of this method were:

- Measures to develop several alternative models of protected IF in the DLS circuits.
- Measures for the development or selection of an adequate optimization model of the LMS IS.
- Search for the extremum of the objective function in the analysis of alternative sets of DLS protection tools, etc.

In particular, as part of the development of a method for justifying measures to ensure the IS of the DLS by the criterion of an integral loss minimum, such a model was proposed to find the optimal values of the periods for reviewing measures aimed at ensuring the IS of the DLS of the university.

If it is necessary to justify the review period for measures related to the provision of IS of the DLS (and/or DEEU) is Δt_0, it is necessary to solve the following system of equations:

$$\begin{aligned} & IL_0(\Delta t_0, T) = \min_{k \in AL} \int_0^T L_k(\Delta t_k, t)dt, \\ & L_k(\Delta t_k, t) = TC_k(\Delta t_k, t) + RV(t) \cdot P_{TR_k}(\Delta t_k, t), \\ & P_{c_k}(\Delta t_k, t) \geq P_g, \\ & P_{TR_k}(\Delta t_k, t) \geq P_{per}, \\ & k = 1,2,3,...K. \end{aligned} \quad (2)$$

where AL is area of permissible time periods for reviewing measures for the IS of the DLS;

$L_k(\Delta t_k,t)$ is the resulting losses at the k-th value of the review period associated with the IS of the DLS at a point in time t;

$TC_k(\Delta t_k,t)$ is total costs for IS of the DLS at the k-th value of the period, for example, can be determined depending on the strategy of investing in IS systems chosen by the university management. Such models are presented in detail in [18, 19];

$RV(t)$ is the value of protected information resources presented in the DLS or DEEU;

K is the number of possible values for the review period for IS activities of the DLS and/or DEEU;

$P_{ck}(\Delta t_k,t)$ is probability of authorized access to IR in DLS;

P_g is the value of the probability of authorized access to IR in the DLS allowed by information security metrics;

$P_{TRk}(\Delta t_k,t)$ is the value of the probability of realization of the IF or processes; violation at the k-th value of the review period of the IS activities of the DLS at the time T;

P_{per} is admissible value for the probability of violation of IF or processes in the DLS.

In this case, you can get a solution that allows to achieve the minimum integral losses on the time interval is $IL_0(\Delta t_0, T)$.

Taking into account the structural features of the protected information flows and processes in the DLS, the value of the protected information resources, the potential awareness of intruders, there is proposed a model that develops the Shewhart-Deming cyclic control model.

4. Conclusions

The following results were obtained in the research:

- A structure for organizing information flows (IF) in distance learning systems (DLS) of universities is proposed, which is able to increase the efficiency of the complex interaction of both existing and new promising mechanisms for controlling and processing IF that circulate in the DEEU and DLS.
- The proposed additions imply the development of new or the use of ready-made models of the protected IF and processes with DLS. And besides, the features of optimization measures related to the information security of the DLS are taken into account. The proposed model covers a set of conditions and tasks that are priorities in the search for optimal information security measures for DLS.

5. References

[1] S. Aljawarneh, A Web Engineering Security Methodology for E-Learning Systems. Network Security, vol. 3, 2011, pp. 12–15.

[2] Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, 2021, pp. 257–264.

[3] Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of Social Engineering Attack at Institution of Higher Education, in: Proceedings of the 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654, 2019, pp. 155–164.

[4] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System, in VI In-ternational Scientific and Practical Conference Problems of Infocommunications. Science and Technology, 2019, pp. 39–44. doi: 10.1109/PICST47496.2019.9061376.

[5] S. H. Hasan, D. M. Alghazzawi, A. Zafar, E-Learning Systems and Their Security, BRIS Journal of Adv. S&T, vol. 2, 2014, pp. 83–92.

[6] L. B. A. Rabai, N. Rjaibi, A. B. Aissa, Quantifying Security Threats for E-Learning Systems, in International Conference on Education and e-Learning Innovations, 2012, pp. 1–6.

[7] A. Blanco-Justicia, et al., Achieving Security and Privacy in Federated Learning Systems: Survey, Research Challenges and Future Directions. Engineering Applications of Artificial Intelligence, vol. 106, 2021, 104468.

[8] C. Savulescu, et al., Security in E-Learning Systems, in 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2015.

[9] L. A. Alexei, A. Alexei, Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning, International Journal of Scientific and Technology Research, vol. 3, 2021, pp. 128–133.

[10] D. Koller, N. Friedman, Probabilistic Graphical Models. Principles and Techniques, MIT Press, 2009.

[11] G. Rajaboevich, N. Nasrullaev, D. Fayzieva, Methods and Intelligent Mechanisms for Constructing Cyberattack Detection Components on Distance-Learning Systems, in 2020 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2020.

[12] D. Dang-Pham, et al., Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems, 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), IEEE, 2020.

[13] N. Rjaibi, et al., Mean Failure Cost as a Measurable Value and Evidence of Cybersecurity: E-learning Case Study, International Journal of Secure Software Engineering (IJSSE), vol. 4.3, 2013, pp. 64–81.

[14] T. Nguyen, V. Reddi, Deep Reinforcement Learning for Cyber Security, in IEEE Transactions on Neural Networks and Learning Systems, 2019.

[15] A. Ahmed, et al., Teaching Cyber-Security for Distance Learners: A Reflective Study, in 2020 IEEE Frontiers in Education Conference (FIE), IEEE, 2020, pp. 1–7.

[16] A. Elsawy, O. Ahmed, O., E-Learning using the Blackboard System in Light of the Quality of Education and Cyber Security, International Journal of Current Engineering and Technology, vol. 9, no. 1, 2019, pp. 49–54.

[17] O. Keskin, et al., Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study, in ICCWS 2018 13th International Conference on Cyber Warfare and Security, vol. 343, 2018.

[18] D. Lakhno, et al., Methodology for Placing Components of a Video Surveillance System for Smart City Based on a Composite Cost Optimization Model, Lecture Notes in Networks and Systems, vol. 501, 2022, pp. 13–23.

[19] V. Lakhno, et al., Modeling and Optimi-zation of Discrete Evolutionary Systems of Information Security Management in a Random Environment, Smart Innovation, Systems and Technologies, vol. 269, 2022, pp. 9–22.