INFORMATION SECURITY ISSUES IN A DISTRIBUTED INFORMATION EDUCATIONAL ENVIRONMENT

A.S. Minzov[a], N.A. Tokareva[b], E.N. Cheremisina[c]

Dubna State University, Universitetskaya 19, 141980, Dubna, Russia

E-mail: [a] 926-565-0570@mail.ru , [b] tokareva@uni-dubna.ru, [c] chere@uni-dubna.ru

Intensive development of computer technology and technologies of distributed computing systems has resulted in the appearance of new active and interactive forms of education. Currently, students have enough opportunities of wide access to electronic educational resources. At the same time, new threats and vulnerabilities have emerged, which can be classified into 3 groups: threats associated with vulnerabilities of portal solutions and information and educational content management systems in a distributed information educational environment; threats related to the relevance, reliability and quality of content presentation; electronic educational resources copyright protection and insufficient regulatory framework for information security. The threats in a distributed information educational environment and mechanisms of information security has been performed.

Keywords: distributed computing environment, education, information security, electronic educational resources

Anatoly Minzov, Nadezhda Tokareva, Evgenia Cheremisina

1. Introduction

More than 20 years have passed since the publication of the article on the concept of individual training in the telecommunication computer educational environment [1], which considered the theoretical, methodological, organizational and didactic problems of introduction of new information technologies and the Internet in the system of professional education. During this period, many achievements have appeared, and a new information educational environment has been created. It allows a significant using electronic educational resources from various sources of the Federal and regional levels: educational institutions and distance learning centers, information resources of various economic entities, funds and electronic libraries, information resources of social networks, electronic archives, private information resources and other sources of information [2]. The advent and mass application of cloud environments made it possible virtual modeling of technical systems, which significantly expanded the possibilities of remote technologies, and the introduction of network interfaces into various technical systems and allowed to include research projects with remote control of equipment in educational processes. Actually, a distributed information educational environment (DIEE) with decentralized management and weak feedback communications has now been established. The standard [3] uses the terminology "electronic information and educational environment", which now, does not reflect the features of information protection in a distributed heterogeneous information and educational environment.

Centralized management of this environment is maintained only at the Federal level and include certain requirements for the metaphysical description of electronic resources. The other information and educational resources are of a referential format and are formed according to various private organization requirements for the forms of presentation of electronic educational resources (EER). The feedback on monitoring changes in information resources, access control, assessment of compliance with their requirements for form and content is practically not provided. This does not allow one to control their quality and relevance.

The educational and information resources of educational institutions of Federal and national research universities, certain universities, distance learning centers and social networking resources are of great interest. However, they are not universal, are built into their distance learning information systems and are often closed or commercial in nature.

A characteristic feature of DIEE is the appearance of new interactive forms of learning based on the simulation of technical, organizational, logistics and other systems in virtual environments, as well as by remote control of technical telemetry complexes with network interfaces.

In summary, concurrently with the appearance of new active and interactive forms of education where students are able to have wide access to the electronic educational resources, the new threats and vulnerabilities have emerged. Thus, it is necessary to analyze threats, to identify the typical ones and propose the mechanisms to ensure information security.

2. Analysis of the current state of information security in distributed information educational environment

The work to standardize the development, implementation and maintenance of EER has begun since 2011. The results of this work are implemented in the standards [3-7], but they are generic in nature and do not fully reflect the current trends in the creation of information and educational environment. They practically have no requirements for information security of EER and control systems except for GOST R 577723-2017 [3] describing the requirements for the security of electronic library systems. At the Federal level, all responsibility for ensuring the safety, relevance and quality of the EER rests with author of the EER, and no functions are performed to control the EER information security when introducing it in the register.

These circumstances have led to the fact that the existing distributed information educational environment in Russia has become very vulnerable to threats of information security. The active implementation of information and educational resources for all education forms require a more

serious attitude to the issues of information security. This is evidenced by the statistics of information security incidents in relation to DIEE [8, 9].

An equally important role in the digital economy is played by the interpenetration of information technologies (web services, telecommunications and information systems, artificial intelligence technologies, Big Data, neural networks, blockchain and other advanced technologies) and information security systems. These trends are reflected in modern concepts of development of the complex systems aimed at results [10]. The vulnerabilities appear at the intersections of technologies, providing new opportunities for cybercriminals to hybrid attacks by exploiting the vulnerabilities of different technologies [9]. Thus, the further development of the quality managed information and educational environment is impossible without creation of the system of certain policies on the confidentiality, integrity, availability, reliability, quality of the EER and copyright protection of developers.

The analysis of the normative documents used at the Federal level of DIEE [3-7], as well as responses and comments of the users of information and educational resources [2] reviles that there are several problems directly related to the information security of the DIEE. Let's focus on some of the DIEE threats and vulnerabilities, which we have considered regarding the educational content of EER and the information security. Based on the user's reviews, the most significant threats are: the presence of malicious code in the loaded EER; the irrelevant (outdated) information in the EER; the modified (false and incorrect) information, which is sometimes introduced artificially; the lack of scientific description of problems, novelty, statements of unsolved problems; the incorrect presentation of mathematical descriptions and models, schemes, graphs, diagrams, presentations, etc. These threats to the quality of the educational process depend largely on the lack of the information security policies to EER and their management system.

Nevertheless, there are regulatory documents in the system of standards in the field of DIEE that deal with certain issues of information security of electronic library systems (ELS) [3]:

a) The requirements for copyright protection of the ELS are defined, but the requirements for the correct inclusion of matching content and compilations of materials from other sources are not specified.

b) There are requirements to the operator of ELS on confidentiality and transfer conditions of content to the users in coordination with the right holder.

c) The rights of the operator of ELS for long-term preservation of archival data of funds of reserve and insurance copies without infringement of copyrights are defined. In addition, the operator is responsible for content integrity violations and the usage of system vulnerabilities, but the mechanism of this responsibility is not defined.

d) There are established the rights of copyright holders to access statistics of their content use and access termination after the expiration of the license agreement.

e) In case of uploading content to user-end devices for offline, the right holder should be provided with the control tools: statistics of downloads, ensuring the deletion of data after the specified period of content use, etc.

f) The access to ELS should be carried out in compliance with the personal data legislation and the restrictions imposed on information of an extremist nature or containing state secrets, as well as with the other restrictions of the Russian Federation legislation.

g) The provision of information resources and ELS services must comply with the legislative norms on information security, including the protection of children from the information that harms their health and development.

The analysis of these requirements to the ELS shows that they are general in nature and do not provide a trusted environment in the field of information security for any parties of the educational process (student, university administration, teacher, information or educational resource license holder, administrator, methodologist and other ones). The approach to determination of the requirements is not systematic and is not based on the analysis of the DIEE vulnerabilities and possible threats.

3. Typical vulnerabilities of distributed information educational environment and recommendation on security mechanisms

Considering the inconsistencies described above, we have identified the following main typical DIEE vulnerabilities, which are either not mentioned in the list of requirements for the ELS or are occurred as a result of carrying out the functional requirements for the ELS [3]. Special mention should go to the following:

1. The DIEE vulnerabilities based on the portal solution implementation errors.
2. The vulnerabilities of the educational and information content management systems (LMS).
3. The reliability of the information and educational resources.
4. The ability to include malicious code in the information and educational content.
5. The possibility to include undocumented features in the special DIEE software.
6. The lack of control over the actions of the parties of educational process.
7. The lack of the system for monitoring the integrity of information and educational content and the mechanisms for updating it.
8. The lack of the information security mechanisms in remote control systems of technical telemetry complexes with network interfaces.
9. The lack of the mechanisms in DIEE to protect the intellectual property of the EER authors and to control for plagiarism in content.
10. The lack of a unified system of requirements for the description and presentation of the EER, including in active and interactive forms of learning.
11. The lack of mechanisms for the safety transfer, exchange and other forms of the EER usage between the parties of the educational process in DIEE.
12. The lack of sufficient regulatory framework for the creation, implementation and certification of the EER information security system.
13. The vulnerabilities related to the personal data security of all parties of the educational process.

Of course, these are not all problems of information security in DIEE and it should be assumed that with the increase in the value of the information and educational resources, the interest in them from attackers will significantly increase. There are different methods to solve these problems. Some of them (items 1 and 2) will require the application of recommendations to reduce the vulnerabilities in the development of portal solutions [14] and to expand the knowledge base on LMS vulnerabilities [15]. Items 4 and 5 will require mandatory EER monitoring for malicious code and analysis of the software undocumented features. Properly LMS settings will provide the solution for item 6. The inclusion the integrity control mechanisms for EER in the software structure will be the key in the issue in item 7. The organizational arrangements will be required to address the problems identified in items 9-12. The issue in item 13 needs the development of the personal data information security systems in accordance with the requirements of regulatory documentation [12, 13]. In the existing systems, it will be, as a rule, the 4th level of personal data protection.

We should nevertheless point out that there are some items in the presented list of problems, the solution of that will require considerable efforts and is not a trivial task. We would like to discuss them in more detail.

The ensuring reliability of the presentation of information and educational resources (item 3) in the context of DIEE has a slightly different meaning than that currently used in information security systems. In fact, in the information security systems we create a mechanism of reliability by the source of information, not by the content of information itself, which is much more complicated and can hardly be fully automated at this stage of the development of information security management systems. In our opinion, the educational content should contain information that is safe for the learners, and reflecting the modern, generally accepted scientific representation of the studied issues. The educational content should not contain pseudoscientific theories and artificially introduced concepts and definitions or if case these ones are still presented, they should have a critical form of the presentation. The formalized description of the content must be presented in evidence-based form, not axiomatic. The mechanism to ensure the reliability of the information in DIEE should be reflected in the normative documents for the development of the EEE and define the responsibilities of authors and reviewers. It is also very important to create the educational content monitoring system to provide

reliability of the information as when the EER is included in the DIEE and in the process of its use and updates. Item 8 refers to vulnerabilities in the remote-control systems of technical telemetry complexes with network interfaces. It is essential to develop the remote access systems (Remote Labs) with the preservation of all the basic functions of each device working in the stand and to create the effective network protection system based on WAN and LAN connections [11].

4. Conclusion

Currently, there are several basic concepts of the information security around the world, which differ in relation to the level of the information confidentiality, or are based on the different methods of the information security threat measuring, but in all cases the same trend persists: the more complex the information system is, the more vulnerabilities it has and the more difficult is to protect the information in it. The existing regulatory framework largely reflect only functional requirements for the distributed information and educational environment that is heterogeneous in forms, content and management system and largely leave aside the issues of information security. The presented research has demonstrated the need for the development of normative documents on creation of the information security system in DIEE. The analysis of typical vulnerabilities has been carried out and the mechanisms for protecting information and creating a trusted security environment have been proposed.

References

[1] Minzov A. S. Kontseptsiya individual'nogo obucheniya v telekommunikatsionnoy komp'yuternoy obrazovatel'noy srede [The concept of individual learning in a telecommunication computer educational environment]//Distantsionnoye obrazovaniye. – 1998. №. 3. S. 19-22.

[2] Osnovnyye polozheniya kontseptsii sozdaniya sistemy obrazovatel'nykh portalov. Internet-portaly: soderzhaniye i tekhnologii [The main provisions of the concept of creating a system of educational portals. Internet portals: content and technology]: sb. nauch. st. Vyp. 1. / redkol.: Tikhonov A.N. (pred.) i dr. / GNII ITT «Informika». M.: Prosveshcheniye, 2003. 720 s.

[3] GOST R 57723- 2017 Informatsionno-kommunikatsionnyye tekhnologii v obrazovanii Sistemy elektronno-bibliotechnyye. Obshchiye polozheniya [Information and communication technologies in education. Electronic library systems. General Provisions]. M.: Standartinform, 2017.

[4] GOST R 53620-2009 Informatsionno-kommunikatsionnyye tekhnologii v obrazovanii. Elektronnyye obrazovatel'nyye resursy. Obshchiye polozheniya [Information and communication technologies in education. Electronic educational resources. General Provisions]. M.: Standartinform, 2011.

[5] GOST R 55750-2013 Informatsionno-kommunikatsionnyye tekhnologii v obrazovanii. Metadannyye elektronnykh obrazovatel'nykh resursov. Obshchiye polozheniya [Information and communication technologies in education. Metadata of electronic educational resources. General Provisions]. M.: Standartinform, 2014.

[6] GOST R 55751-2013 Informatsionno-kommunikatsionnyye tekhnologii v obrazovanii. Elektronnyye uchebno-metodicheskiye kompleksy. Trebovaniya i kharakteristiki [Information and communication technologies in education. Electronic training complexes. Requirements and specifications]. M.: Standartinform, 2014.

[7] GOST R ISO/MEK 2382_36 - 2011 Informatsionnyye tekhnologii. Slovar'. Chast' 36. Obucheniye, obrazovaniye i podgotovka [Information technology. Vocabulary. Part 36. Teaching, education, and training]. M.: Standartinform, 2012.

[8] Aktual'nyye kiberugrozy I kvartal 2018 goda [Actual cyberthreats I quarter of 2018]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q1/#Obrazovaniye (accessed 27.07.2019).

[9] Simis Boris Kiberbezopasnost' — 2018−2019: itogi i prognozy [Cybersecurity - 2018−2019: results and forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/ (accessed 27.07.2019).

[10] COBIT 5: Biznes-model' po rukovodstvu i upravleniyu IT na predpriyatii. [COBIT 5: Business model for the management and management of IT in the enterprise]. Available at: http://www.wikiitil.ru/books/Cobit-5_frm_rus_0813.pdf (accessed 27.07.2019).

[11] Kryazhenkov K. G. Setevyye obrazovatel'nyye resursy [Network educational resources] // Obrazovatel'nyye resursy i tekhnologii. 2015. №. 1 (9).

[12] Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 01.11.2012 g. № 1119 «Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [Decree of the Government of the Russian Federation dated 01.11.2012 No. 1119].

[13] Prikaz FSTEK Rossii ot 18.02.2013 g. № 21 «Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» [Order of the FSTEC of Russia dated February 18, 2013 No. 21].

[14] Special Publication 800-95. Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology.

[15] Bank dannykh ugroz i uyazvimostey FSTEK [The FSTEC databank of threats and vulnerabilities] Available at: https://bdu.fstec.ru/vul (accessed: 27.07.2019).