TECHNOLOGICAL ORGANIZATION OF THE ACCESS MANAGEMENT TO INFORMATION RESOURCES IN A COMBINED E-LEARNING ENVIRONMENT

Radi Romansky, Irina Noninska

Technical University of Sofia
e-mails: rrom@tu-sofia.bg; irno@tu-sofia.bg
Bulgaria

Abstract: The article deals with technological organization and functional features of a combined e-learning environment based on social and cloud computing. Two subsystems are determined for user access and requests processing with discussion of the principles of access regulation to different information resources. The role of the e-learning management system which supports procedures for correct registration, identification, authentication and authorization is determined. A summarization of possible security problems is made in the last section of the paper.

Key words: combiner e-learning, cloud services, access management, information security, privacy and data protection.

1. INTRODUCTION

The globalization in the contemporary digital age outlines new important challenges in privacy and personal data protection which reflects to the applied principles of user's security in the cyberspace and determines the cyber security policy in the European Union [1]. This is valid not only for the public sector and administration, economic life and defence sector, but also for digital communication and remote access to the information resources of each e-learning environment where distributed educational materials via the global network are used [2]. It is known that distributed processing of data has its own specific requirements for the management of the access to resources, including strong regulation based on the rights for using by an e-Learning Management System (eLMS). The contemporary Information and Communication Technologies (ICT) propose new opportunities for e-learning processes' realisation but they create new challenges for the privacy of tutors, students, administration staff and all other participants [3]. Yes, the information sharing is a good form of relation between users in the global world. On the other hand, the contemporary technologies as social computing, cloud services, mobile cloud applications, Internet of Things (IoT), Cyber Physical Systems (CPS),

Big Data Analytic, etc. permit extending the functionality of e-learning environments by new, sophisticated relations and opportunities. Each of these technologies could be used to develop different types of combined e-learning architectures with a virtual structure and features [4].

The article deals with organization and functional features of combined e-learning environment (CeLE) based on social and cloud computing [5] and discus some important principles of access regulation to different information resources. Two types of resources are supported in discussed CeLE – internal resources (stored in its own stations and accessed via internal local network) and external resources (by using social networks, blogs/microblogs, cloud, etc. and accessed on the base of the global network communications). On the other hand, all these resources could be determined in two main directions: as public (without protection of the access) and private (with strong regulation of the access). There are hierarchical levels of the eLMS for access management to the second type resources based on the procedures for registration, identification, authentication, authorization and data protection. In this reason, the article presents a point of view about technological organization of CeLE by using the ICT of the 21st century for increasing the effectiveness of e-learning processes. A structure based on two sub-systems (front office and back-office) is described and the functionality of eLMS is discussed. A summarization of possible security problems is made in the last section of the paper.

2. A BRIEF SURVEY OF THE E-LEARNING DEVELOPMENT

It is fact, that the network communications and the digital technologies are the reason for extension of the e-learning area, but the idea for non-traditional education and training is not new. The good presentation of the history is made in [6] where the middle of 19th century is marked as the beginning of non-traditional forms of education developing, started by the student distance courses proposed by Isaac Pitman in 1840s, and organized on the base of post correspondence. The 20th century is characterized with machine automation of selected parts of the learning process – machine self-testing by students (1924), developing “Learning machine” to help the educational administration (1954), introducing computer-based training programs (1960s), etc.

The last 3 decades of the 20th century are characterized by creating the first online education system (1970s) and using personal computers in the learning processes (1980s), but the creation of hypertext technology and the emergency of the Internet as the main global network for communication between people “opened door” for new attractive forms of remote access to information resources, virtual learning environments, distance online courses, etc.

The term "e-learning" was used in year 1999 as an alternative of the concepts "online learning" and "virtual learning". The new technologies of 21st century and the globalization of the society enabled the transformation of e-learning to create new innovative forms as micro-learning (small steps for education in digital media

environment forming separate sessions) [7], gamification (including gaming mechanism for developing educational content) [8], personalized learning (for supporting learners with specific needs) [9], etc.

Extension of the e-learning technology can be presented by the other forms as d-learning (distributed learning), m-learning (mobile learning), etc. (Fig. 1). As a next phase could be determined the combination of the traditional forms of e-learning and the extension of the m-learning with the opportunities of the cloud computing – new from called in advance "c-Learning" [10].

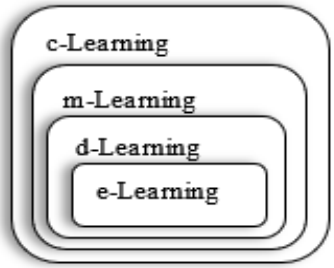

Figure 1. E-Learning extension

The cloud learning (c-learning) permits learning resources using by distributed access and allows the application of cloud principles and services in the learning processes. This permits a part of the information resources to be stored in the cloud and to design virtual learning environments. For example, [11] discusses such environment designing as a possibility "*to improve the quality of teaching and learning processes in higher education*" by using ICT to "*integrate different open source tools … and developed tools to support administration, monitoring and assessment*". However, the need to take strong security measures must be taken into account, so [12] discusses necessity of risk analysis when cloud services are used. This article proposes "*a risk assessment approach for assessing the potential damage from the attack on the implementation of components of confidential data and justify the need for the inclusion of private clouds with a high degree of protection in a hybrid cloud computing environment*". Another publication confirms that the use of different ICT, including cloud services, to support educational processes provides certain advantages and new opportunities, but "*a number of security issues arise, the solution of which may affect the use of cloud technologies*" [13].

An extension of the c-learning a combined e-learning environment (CeLE) could be building on the base of technological collaboration of e-learning principles and structures with the technologies of social and cloud computing, wireless networking, mobile cloud computing and smart technologies. For example, the use of social networks allows active communication between students and teachers, which will replace the classroom. Collaborative learning is based on the principle of sharing learning experiences by each student in the group, being responsible for the actions of others in team work. In addition, the use of external storages of data (data centres) for information, education and selected administrative resources on the base of cloud services will increase the impact of the educational processes' organization and their effectiveness. It should be bear in mind that these new opportunities will increase the importance and the functionality of the Learning Management Systems (LMS) which must support the procedures for internal and external access regulation, strong registration, authentication and authorization [4]. In this reason,

the design of LMS must be made on the base of preliminary formalization by using suitable mathematical apparatus and model investigation to evaluate the efficiency of the projected activities, components, procedures, information resources and different structures [5].

3. FUNCTIONALITY AND ORGANIZATION OF A COMBINED E-LEARNING ENVIRONMENT (CeLE)

Cloud Computing is a distributed environment constructed on the base of connected virtual computers with dynamic communication for provision of computing services. The cloud technologies permit dynamic transition to new forms of education and access to educational and information resources at anytime and anywhere, including by dividing the rights of different users' groups to use resources. The main components and functional features of a collaborative environment for using cloud services in the e-learning are generalized in Fig. 2.

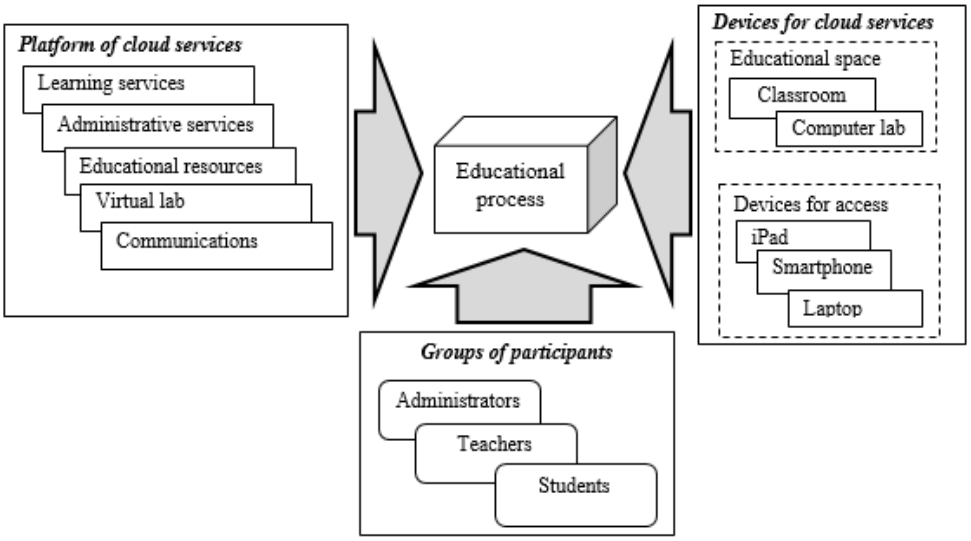

Figure 2. Organization of a collaborative "e-learning & cloud" environment

The development of a CeLE should be made on the base of preliminary determination of a suitable architecture as a collection of some partially independent sub-systems to support the system functionality. Two sub-system for the processes supporting should be designed as a basic composition of the CeLE architecture – input portal (front office) for external users' access and administrative part (back office) for realization of the processes.

Another component of the architecture that need to be planned is the collection of all resources that will support all educational processes (educational, information

and administrative). This third part of CeLE will collect internal resources (stored in their own memories) and different external resources (stored in the cloud, web sites, blogs and microblogs, etc.). Both types of information resources must be provided with the necessary organizational and technological measures for information security, including personal data protection based on the requirements of the European regulation GDPR [14]. In this respect, a specific data model [15] could be used to provide reliable information support.

The primary responsibility for protecting all information resources is given to the eLMS (e-Learning Management System) which is realized by hierarchical levels of the procedures for registration, identification, authentication and authorization. Important tasks of this systems are as follows: ✓ Limiting third party access to the server; ✓ Minimization of the categories of collected personal data of the users (students and teachers) and applying the paradigm "right to be forgotten/ to be erased"; ✓ Controlled registration of new information in the system from authorized persons only; ✓ Applying the principles "privacy by design" and "privacy by default" introduced by the GDPR; ✓ Supporting copies of the important data and critical information resources in a place different from the traditional using; ✓ Taking suitable measures to limit damages after the possible security breach.

The general organization of the first sub-system (Front Office) is shown in Figure 3. This is the input point for connection of users to the cloud which is realized by using web browser with a standard address (IP address or domain).

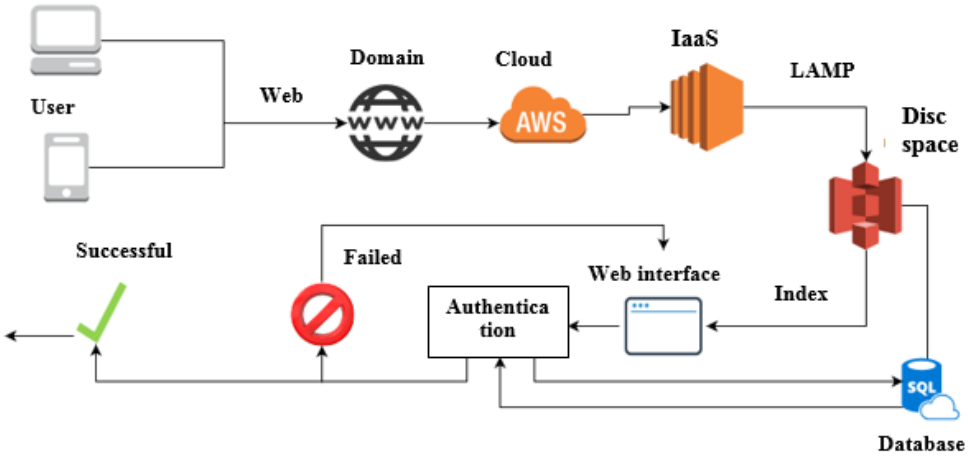

Figure 3. Organization of a Front Office of the e-learning managing system

The access to the system could be made by a domain. This corresponds to the leased cloud infrastructure (IaaS). Installation of a server in such infrastructure must be made for accessing the program system of the CeLE and this could be realized on the base of software package LAMP (Linux – Apache – MySQL – PHP). The main

functions of the front office are realized after access to the disc space and are supported by Index File & Web interface (input of personal data for preliminary registration) and procedure for authentication (to determine the legitimate user's access). Only positive result of the authentication will permit input in the Back Office sub-system (Figure 4).

Another function of the Front Office sub-system is the collection of statistics for all inputs in the system (successful and unsuccessful) and registration in the related database supported on the disc space. This function should limit the number of unsuccessful attempts for each user with possibility for blocking the access to counter attempts at Brute Force attacks or attempts to hack users and their passwords. For the purposes of maximum system security, the users are not able to open their own accounts, so only the authorized administrator can access personal data.

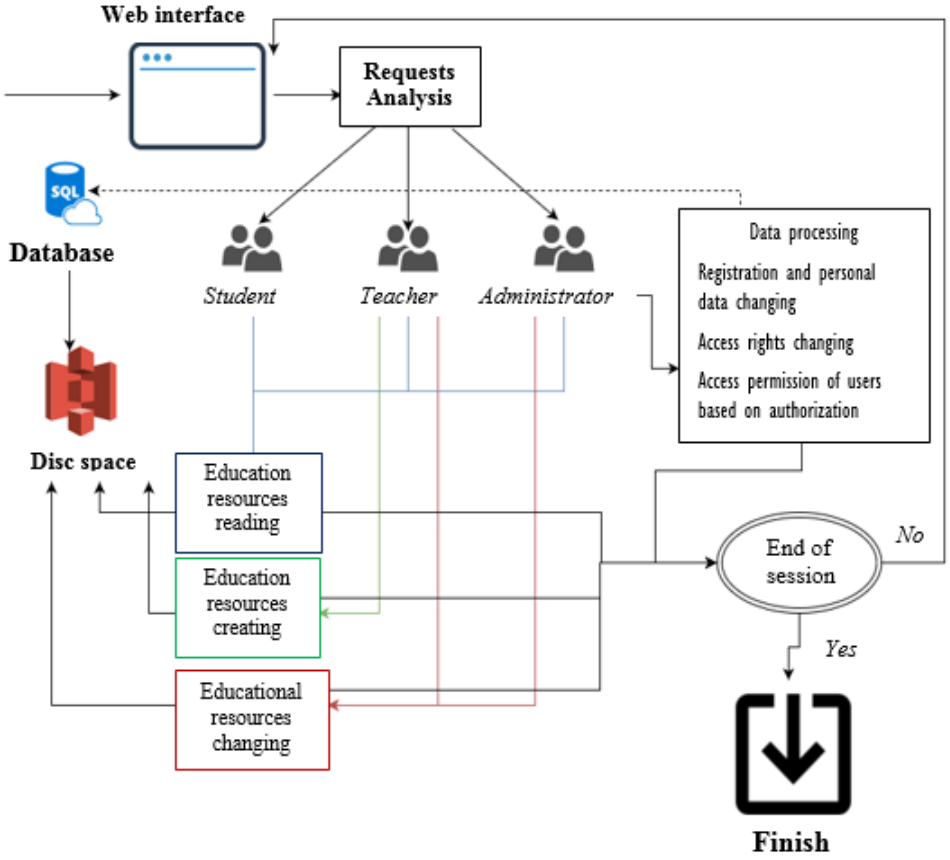

Figure 4. Functionality of a Back Office subsystem

The Back Office subsystem (Figure 4) processes the legitimate request received from the Front Office subsystem on the base of principles "CIA"

(Confidentiality, Integrity and Availability), realized by Digital Rights Management System (DRMS) as an important part of the eLMS. Main features of the system can be summarized as follows:

✓ Initial request analysis to determine the source (teacher, student or administrator) and the type (to select appropriate procedure for servicing). If the request is intended to access an external resource, the user should be transferred to this object after preliminary security checking. Such manner is used in some social networks (Facebook, for example);

✓ An internal resource could be accessed after preliminary processing of the request with the right level determining and user's authorization checking. The administrator has the highest authorization level and rights to register new users, to delegate rights and to control the access to all resources in the system. The teacher has the next level of rights which as distinct from the student can create new educational and information resources and make changes in the existing ones (each teacher has access to his/her own resources only);

✓ The disc space is a virtual information environment which contains all information, education and administrative resources (including profiles of personal data). A hierarchical organization is made, and the regular user has access only to first level without access to the working functions and files of the eLMS in order to counter cyberattacks;

✓ Database – it contains information for the users, resources, access rights, defined per different groups. They are user's profiles; groups of users; rights of users; existing pages; rights of user's group for page accessing; web site configuration information; statistics; educational resources; categories (lectures, labs, etc.).

4. POSSIBLE SECURITY PROBLEMS IN A COMBINED E-LEARNING ENVIRONMENT

The possible security problems in a combined e-Learning environment could be specified in two main directions – privacy and information security. The first direction is related to the protection of the collected personal data of all participants in e-learning processes supported in the CeLE, including communications with the cloud. Different digital technologies (as social networks and cloud services) used in CeLE may lead to more personal data being entered that necessary and this could be a problem for the user's privacy. The required personal information collected during the registration must be limited to those data, which are used by e-learning processes excluding sensitive and quite specific data. All procedures related to personal data collection and processing, including transfer to third parties, must be clearly determined and presented in a special section "Privacy policy" in the input portal of the Front Office subsystem. They must realize the basic principles of personal data correctness specified in the European regulation GDPR: ✓ Lawfulness; ✓ Good faith and transparency; ✓ Goal limitation; ✓ Minimization of data collection; ✓ Accuracy; ✓ Limited keeping (storage); ✓ Integrity and confidentiality;

✓ Accountability. The further processing of personal data is permissible in the following cases: ✓compatibility with the purpose of primary processing; ✓ for additional purposes with the consent of the person or the existence of a legal norm.

It should be specified that the processing of personal data is lawfulness at:

✓ Consent of the person for one or more specific purposes;

✓ Availability of a contract;

✓ Legal responsibility of Data Controller;

✓ Protection of the vital interests of the individual or other individuals;

✓ Task performed in the public interest or in the expertise of official authority granted to the data controllers;

✓ Legitimate interests of a data controller or a third party, when they have an advantage over the interests and rights of the data subject.

The owner of the CeLE is determined as a Data Controller with concrete obligations summarized in the GDPR. The importance of these obligations increases when social and cloud computing are used, because some difficulties could be defined, for example: ✓ difficulties with data processing roles' identification in the social/cloud space; ✓ impossibility to guarantee all rights of the user in terms of data owner; ✓ multiple data transfer between different locations via the Internet; ✓ lack of actual information for organizational and technical measures that are used for personal data protection.

The goal of the second direction is to keep information accurate and protected of unauthorized access, including personal data too. The use of technologies and tools of social and cloud computing imposes additional security requirements. The possible risks of storing data in the cloud are related to the confidentiality of information that can be compromised by the principle of multitenancy, the availability of copies of data in different nodes, possible periodical transfer of data between different nodes, etc. Some advantages and disadvantages of the collaboration between e-learning and cloud computing are summarized in Table 1.

Table 1. Advantages and disadvantages of cloud technology using in e-learning

Advantages	***Disadvantages***
✓ Large Infrastructure Management; ✓ High wear resistance; ✓ Provision of information protection of resources; ✓ Good data processing speed; ✓ Reduced cost of equipment and maintenance; ✓ Disk Space Savings, etc.	✓ Dependence on the availability and quality of communication channels; ✓ Dependence on the rules for the protection of user data provided by cloud services; ✓ The emergence of new ("cloud") monopolies; ✓ Risk of technical damage; ✓ Legal issues to solve.

Some of the most common attempts to breach information security are as follows.

Brute force attacks (attempt at guessing) – this is an attempt to guess the user's password by using a previously prepared list of possible ones. Counteraction to this type of attack can be accomplished by using "strong" (complex) passwords and/or by including specific question and typing fixed answer.

SQL Injections – an attempt to enter data into information structures which will be activated as program code allowing unauthorized access to protected resources. A proper solution is to limit strictly the possibility of external access to the system.

Malware Installation – the purpose of this attack is to install malicious software on a computer allowing access to the system resources and to protected data. The prevention is to restrict the access to the important and sensitive information only to limited number of selected persons who cover the required authorization level.

Attempts to capture authentication data – enticing a user to issue (inadvertently) and share confidential parameters for e-identification in order to access sensitive information (username, password, credit card details, etc.). The user is offered to enter into a false environment where he/she makes his authentication with his/her real data, which can be done through the following

- ✓ *E-mail* sent by bank, financial institution, internet provider, social network;
- ✓ *Spear phishing* – e-mail in unified form on behalf of a known person or a known company such as eBay or PayPal with an instruction for account registration or account update;
- ✓ *Phishing e-mail* containing an official logo or other distinguishing sign of an institution (taken from an official website) for the conviction of the contact;
- ✓ *Reference* to masked, fraudulent Web sites resembling the original, asking for input of personal information (an example is shown in Figure 5):
- ✓ *Phone Phishing* – e-mail requesting a phone call (determined as a support) claiming that the registration will be terminated or there are some problems with it.

Figure 5. An example of a masked address
(when the cursor is placed, the real address appears)

Since the number of mobile devices grows, the number of attacks on them increases, with new types of attacks such as: *vishing* – mobile phone phishing; *smishing* – phishing by sending SMS (smishing is when an attacker tries to trick an user into giving his private information by sending him a text or SMS message). There are applications such as SMS-blasting (sending a message with a phone number to return the call) and SMS-spoofing (sending a SMS with a link for updating the personal profile).

A summary of information security breaches is presented in Table 2.

Table 2. Information security breaches

Group	***Breaches***
1) Channels for information leak	✓ Direct theft of a disk medium; ✓ Copying the information from a medium; ✓ Unauthorized connection to an information system or communication channel; ✓ Unauthorized access to information by special means; ✓ Electromagnetic wave interception from apparatus.
2) Major violations:	✓ Audition without disturbing the operation of the system; ✓ Changing the settings and the state of the system; ✓ Disguise of one logical object as another, possessing greater powers; ✓ Blocking a logical object to prevent some messages from being blocked; ✓ Re-addressing messages; ✓ Modification of messages and others.
3) Problems at the information security breach	✓ Attacks on financial systems; ✓ Discretization of the activities of corporations; ✓ Disclosure of corporate secrets; ✓ Sabotage of production processes; ✓ Breach of intellectual property rights; ✓ Illegal disclosure of personal data.

5. CONCLUSION

The role of the digital technologies in the Information Society increases continuously and their using in the e-learning environments will improve the effectiveness of the education and training. Development of the new forms of e-learning must be tailored with the security requirements for information resources protection and strong access regulation. In this reason, the article discusses the main principles which must be in the fundamental concept at the CeLE organization. The proposed approach determines two relatively independent subsystems with their own tasks for ensuring reliable security protection. This allows to allocate obligations, procedures and tools between these two parts according to their importance and significance. The future research in this field could be to extend the scope of the information resources, supported by a CeLE determining them in different groups (public, private, personal) and to specify concrete measures for their protection. It is very important to determine the manner of these resources storing (on external or on internal memories) which will define the suitable procedures for protection, rights for access, levels of authorization, etc.

REFERENCES

[1] Kovacs, L., Cyber Security policy and the Strategy in the European Union and NATO. *Land Forces Academy Review*, **No. 1 (89)**, vol. XXIII, 2018, pp. 16-24. Available at: https://www.degruyter.com/downloadpdf/j/raft.2018.23.issue-1/raft-2018-0002/raft-2018-0002.pdf

[2] Udroiu, A. M. Implementing the Cybersecurity Awarness Program Using e-Learning Platform. "*Conference proceedings of "eLearning and Software for Education (eLSE)*", **14**, April 2018, pp. 101-104

[3] Adejo, O. W., I. Ewuzie, A. Usoro, T. Connolly. E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastucture. *International Journal of Information Technology and Computer Science*, **4**, 2018, pp.1-9.

[4] Romansky, R. & I. Noninska. Architecture of Combined E-Learning Environment and Investigation of Secure Access and Privacy Protection, Chapter 65 in "*Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*", IGI Global, USA, ISBN 978-1-522-571-131, October 2018 (2174 p.), pp. 1345-1356.

[5] Romansky, R., I. Noninska. Principles of Secure Access and Privacy in Combined E-Learnng Environment: Architecture, Formalization and Modelling. Chapter 9 in the book: "*Multidisciplinary Perspectives on Human Capital and Information Technology Professionals*" (Ed. Vandana Ahuja & Shubhangini Rathore). IGI Global Publ., USA, ISBN13: 9781522552970; EISBN13: 9781522552987, February 2018, pp.152-178

[6] Epignosis LLC. E-Learning Concepts, Trends, Applications, *FREE digital ebook. V 1.1*, San Francisco, California, 2014, pp.69-87.

[7] Giurgiu, L. Microlearning an Evolving eLearning Trend. *Scientific Bulletin, De Gruyter*, **1(43)**, vol. XXII, 2017, pp.18-23 (https://www.degruyter.com/downloadpdf/j/bsaft.2017.22.issue-1/bsaft-2017-0003/bsaft-2017-0003.pdf)

[8] Kim S., Song K., Lockee B., Burton J. What is Gamification in Learning and Education?. In: *Gamification in Learning and Education. Advances in Game-Based Learning*. Springer, Cham, 2018, pp. 25-38

[9] Dockterman, D. Insights from 200+ years of personalized learning. *npj Science of Learning*, **3**, article 15, Sep 2018 (https://www.nature.com/articles/s41539-018-0033-x).

[10] Sanchez, M., J. Aguilar, J. Cordero, P. Valdiviezo. A Smart Learning Environment based on Cloud Learning. International Journal of Advanced Information Science and Technology (IJAST), **39** (vol. 39), July 2015, pp.39-52 (https://pdfs.semanticscholar.org/ad54/c2b60ee658ad92bc0c5c6999ee0ff0690e29.pdf)

[11] González-Marcos, A., R. Olarte-Valentín, E. Sainz-García, R. Múgica-Vidal, M. Castejón-Limas. A Virtual Learning Environment to Support Project Management Teaching. *Proceedings of the International Joint Conference SOCO'17 - CSIS'17 – ICEUTE'17*, Leon, Spain, 6-8 Sep 2017, pp. 751-759. Published in "*Advances in*

Intelligent Systems and Computing", vol 649, 2018. Springer, Cham (https://link.springer.com/chapter/10.1007/978-3-319-67180-2_74)

[12] Tsaregorodtsev, A. V., O. Ja. Kravets, O. N. Choporov, A. N. Zelenina (2018). Information Security Risk Estimation for Cloud Infrastructure, *International Journal on Information Technologies and Security*, ISSN 1313-8251, **No. 4** (vol. 10), 2018, pp. 67-76.

[13] Zaslavskaya, O. Yu, Al. A. Zaslavskiy, V. E. Bolnokin, O. Ja. Kravets (2018). Features of Ensuring Information Security when Using Cloud Technologies in Educational Institutions, *International Journal on Information Technologies and Security*, ISSN 1313-8251, **No. 3** (vol. 10), 2018, pp. 93-102.

[14] Romansky, R. A Survey of Informatization and Privacy in the Digital Age and Basic Principles of the New Regulation. *International Journal on IT and Security* (ISSN 1313-8251), **No. 1** (vol. 11), 2019, pp. 95-106.

[15] Tzolov, Tz. Data Model in the Context of the General Data Protection Regulation. *International Journal on IT and Security* (ISSN 1313-8251), **No. 4** (vol. 9), 2017, pp. 113-122.

Information about the authors:

Radi Romansky is a full professor at Technical University of Sofia, Department of Informatics, Ph.D. in Computer Engineering and D.Sc. in Informatics and Computer Science; Vice Rector of Technical University of Sofia (2015-2019); Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has been a member of Bulgarian Commission for Personal Data Protection (2002-2007). He has over 200 scientific publications and over 20 books. Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, data protection, etc.

Irina Noninska - PhD, Associate professor in Cryptography and data security. She has obtained her PhD degree in Databases and Local Area Networks from Technical University of Sofia. Now she is a lecturer at Computer Systems Department, Technical University of Sofia, delivering courses "Cryptography" and "E-business technologies". Her scientific and research interests are in the area of Information and Network Security, Data Protection, Cryptographic Algorithms and Protocols, Quantum cryptography, Cyber security, Internet of Things, Telecommunication Standards. She is author and co-author of more than 90 scientific papers, articles and 11 books and chapters in books. She is a member of: Union of Scientists, Bulgaria; Union of Automatics and Informatics; International Editorial Board of International Journal on IT and Security; Organizing and Program Committee of Information Technologies.

Manuscript received on 02 October 2019