Introducing Information Security Concepts and Standards in Higher Education

Daniela Orozova [1], Kalinka Kaloyanova [2], Magdalina Todorova [2]

[1] Faculty of Computer Science and Engineering, Burgas Free University, Bulgaria
[2] Faculty of Mathematics and Informatics, Sofia University, Bulgaria

***Abstract* – Information security deals with protecting data and information in all of its forms. The information security topic has been an area of growing research and educational interest for years. Many universities started to incorporate security concepts in new or existing courses, following the recommendations of the ISO/IEC 27000 series of standards. Recently, a new CSES2017 curricula in cyber-security education was introduced.**

The article presents its authors' experience in delivering education in information security area through courses in several Bulgarian universities. The main topics and educational methods, covered by the courses are presented and some results are discussed.

***Keywords* – Information security, ISO/IEC 27001, ISO/IEC 27002, Information Security Management System (ISMS), threat, risk analysis and assessment, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).**

1. Introduction

Information security is a task of global importance as it affects international trade, electronic trade, mobile electronic trade, mobile communication, social media, as well as different systems and services constructing our digital world and national infrastructures. Information security management is an even more complex and difficult task, which involves "using and managing the policies, procedures, processes, control measures and supporting applications, services and technologies that are needed to protect the information that organizations, governments, consumers and citizens rely on to carry out their business and to live their Lives" [1].

The international standards ISO/IEC 27000 were developed in the year 2000, and have been constantly improved since then, in order to meet the needs of the modern business for information protecting.

The ISO/IEC 27000 family of standards provides the basic recommendations for organizations to handle the security of their information assets. ISO/IEC 27001 introduces the concept of Information Security Management System (ISMS) as a systematic approach for effectively managing the security of information. The requirements established by this standard are designed with respect to its compatibility with all types of organizations.

This article presents the authors' experience in integrating the above mentioned standards in information security education in several Bulgarian universities. The discussed education is provided in different programs in Computer Science area at graduate and undergraduate level.

2. Information Access Management and Control as a part of the Information Security Education

The International Standard ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof [2]. The purpose of the ISO/IEC 27001 training is to provide learners with knowledge and skills needed for assessment compliance and effective implementation of ISMS for risk protection of the

DOI: 10.18421/TEM83-46
https://dx.doi.org/10.18421/TEM83-46

Corresponding author: Magdalina Todorova,
Faculty of Computer Science and Engineering, Burgas Free University, Bulgaria
Email: magdalinavtodorova@gmail.com

Received: 29 April 2019.
Revised: 06 June 2019.
Accepted: 14 June 2019.
Published: 28 August 2019.

organizations. This is our motivation for the education in information security area strictly to follow the ISO/IEC 27001 standard, as well as the similar standards for information access management and control.

Information Security courses are provided in most Bulgarian universities - Sofia University, Burgas Free University, Technical University – Sofia, Varna Free University, etc., mostly for the students in Computer Science and Information Technology areas. The courses are provided both for graduate and for undergraduate level – usually at the end of their studies. Also, specialized programs on Information Security were created at graduate level in several universities.

In this paper we will focus on the education in information security area provided in two of the above mention universities – Sofia University and Burgas Free University, which follows similar educational principles. The courses gradually introduce concepts of physical, documental, business and personal security, as well as information systems and networks security. A key element of these courses is the introduction of the standard ISO/IEC 27001 [2]. The standard can be used as a manual for information management, providing good practices and guidelines for information security area. It also is designed for total compliance with other well-known standards, such as ISO 9001 [4], ISO 14001 [5], etc.

3. Basic terminology

The main information security goal is to protect data and information from possible harmful malicious actions, such as: unauthorized access, use, disclosure, alteration, reading, recording and destruction; as well as to minimize the damage in case of such intrusion. Several basic concepts should be noted here:

- *Information security* is defined in [2] as "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved".
- *Computer security* is focused on the particular work of the computer systems and networks, and the information they process. "Computer security is the protection of the items you value, called the assets of a computer or computer system [3]".
- *Information protection* includes: practices of the management of the risks related to using, working, storing and transferring information; the systems and processes used for these.

Information security, computer security and information protection are interrelated and have common objectives, such as: confidentiality, integrity and information accessibility. The last three concepts are defined by the standard ISO/IEC 27001 as follows:

Confidentiality **– "**the property that information is not made available or disclosed to unauthorized individuals, entities, or processes".

Integrity **–** "the property of safeguarding the accuracy and completeness of assets".

Information access **–** "freedom or ability to identify, obtain and make use of data or information effectively".

4. Introducing main concepts in the courses

Usually the information security courses are provided after completing studies in the main topics in the computer science area - operational systems, discrete structures, programming, object-oriented programming, data bases, computer architectures, and computer networks. The courses focus on different risks and threats for the automated information systems and networks, as well as on the actions related to meeting the standards for information security and information protection, which the specialists working in this rapidly developing area need to perform. They introduce the main rules and activities for management and control of the information security, good practices, actions and assessment of key elements in a system based on the ISO/IEC 27001 standard [2].

Basically, the education follows several steps: defining existing and potential threats; identifying the subjects which are prone to threats; risk assessment; getting to know network and computer-oriented systems for intrusion detection/prevention (IDS/IPS); studying current methods and tools for protection from the known threats. Further in this section they are discussed in more details.

4.1. Identifying existing and potential threats

First, main concepts like vulnerability and threat are introduced, as well as different types of threats.

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm as is defined in [3]. More generally speaking, a threat is each possibility of random or deliberate unauthorized access to the created, processed, stored or transmitted information. These are events or actions that endanger an object, and occur in case of existing vulnerability.

A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm [3]. It is a weakness in the system of security measures or in the control of their implementation, which can lead to compromise or facilitate compromising of security. Vulnerability may be a failure, or it can be a result of insufficient monitoring, incomplete or inadequately work organizing, or inefficient physical protection. Vulnerability can be of a technical, software, technological nature.

A threat for an information system can be all objects (passive elements sending or receiving information) or subjects - active elements like a human, process or piece of equipment, which transfer information between objects or modify the condition of an information system or network.

Knowledge about the potential threats, as well as about the vulnerable parts of the information security, creates an opportunity for selecting the most efficient protection tools. During the courses, the students are gradually presented with different types of threats, according to their different characteristics [3]:

- Accidental or intentional threats

Accidental threats are these caused by insufficient expertise in the field. Such threats can be caused by the users or system administrators who have not been properly trained, have insufficient understanding of the documentation, and do not understand the importance of adequate application of protection procedures. For example, a user can try to update a database in an inappropriate manner and can accidentally delete a file. *Intentional threats (attacks)* are these ones caused by malicious people, as a result of whose actions destruction, modification, forgery or disruption of data or data flow can occur. Such threats are: Trojan horses, viruses, worms, etc.

- Direct or indirect attacks

Direct attacks target directly the subject itself. For *indirect* ones, the attacker receives information about the object or objects and subjects associated with it, without attacking the object itself. For example, it is possible to send requests to database processing systems, whose answers include data about the subject, which in turn can be used to draw conclusions about it.

- Active and passive attacks

Depending on the way they act, the attacks can be active or passive. *Passive attacks* are these related to observing the system and collecting data on how it works. The *active attacks* change the behavior of the system in different ways, such as sending messages under false identity; modifying, delaying, changing the sequence, copying or deleting messages or packages; intentional actions against the system software aiming at system breakdown, etc.

- Depending on the subject of attack.

Losing control over the system protection happens when the protection does not function adequately. This may lead the system to reach a state when unauthorized access is possible.

A channel of information breach – this is a situation that designers have not foreseen, or defensive mechanisms can not recognize it as a prohibited state of the system.

4.2. Identifying the subjects which can be subject to a threat

ISO/IEC 27001 [2] identifies the main subjects of threat and all of them are covered in the courses:

Information – it can be stolen, destroyed, altered, blocked or compromised.

Software – it consists of operation systems, applications and services. These are the main targets of the classical attacks and are the main source of system vulnerability. The attacks against them can result in system breakdown, i.e. to complete or partial loss in functionality, and can allow for the attacking party to do unauthorized actions, as well as to control the system.

Equipment and infrastructure elements – it includes servers, active network equipment, network cables, electricity supply, etc. can also be threatened.

4.3. Risk and risk assessment

ISO/IEC 27001 formally specifies an ISMS. It includes a suite of activities concerning the management of information risks (called 'information security risks' in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks [2]. Following the standard [2], the next stage of students' education is dedicated to presenting the process of risk assessment. In order to do this, the following terminology is introduced: risk, risk analysis and assessment, as defined in [2].

The definition of the term risk in the edition of ISO/IEC 27001 from 2013 differs from the one given in 2005. It was worded in more general terms, it is now open to a wider range of methods and techniques for risk assessment.

In ISO/IEC 27001 (2013) "*Risk* is the effect of uncertainty (on objectives) ". The elements of this definition can be interpreted in several ways, so the "effect" can be thought of as the consequences or impact of an event occurring such as the consequences of a malware incident on an email server [1].

The risk in business information systems and networks is a measure for quantitative assessment of the possibility for their vulnerabilities to be exploited towards realization of a threat. As a result, they are harmed in the form of different degrees of compromising their security. When the necessary measures are taken, they have to be checked for efficiency, i.e. the remaining risk to be acceptable. Next, a certification procedure is issued according to the Bulgarian legislation.

Risk appears when there is a threat. As a rule, the presence of a given threat is a result of weaknesses in the security of the information system/network, which can be explained by the absence of particular security programming tools or equipment, or by the defects in the mechanisms that implement them. It is important not only to identify the threats, but also their origin. This can help in choosing additional security tools. After that, risk assessment should be performed [2]. The details in this topic introduced dependence on whether there is a separate course "Risk Analysis and Assessment" at the university [6].

4.4. Systems for detecting/preventing intrusion

The following specific IT security controls and mechanisms are highlighted in [1]**:**

- Network security (e.g., as found in ISO/IEC 27033);
- Applications security (e.g., as found in ISO/IEC 27034);
- Malware (e.g. as found in NIST SP 800-83);
- Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems;
- Access control.

Based on these recommendations, our courses introduce to the architecture and capabilities of the Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS). Both IDS/IPS are part of the network infrastructure. The main difference between them is that IDS is a monitoring system, while IPS is a control system [7]. IDS/IPS systems are dynamic information security systems, as they can identify intrusion and react; for example, they can emit a sound or light signal, email, etc. Some implementations of these systems can email the attacker informing him that he is committing a crime; can switch off the connection with the outside world by a firewall or even attack the attacker.

As IDS/IPS identify the possible incidents and register information about them, stop the incidents and inform the security administrators about them, it is essential for students to understand the importance of these systems, as well as the fact that they are indispensable for each organization infrastructure.

Further, students study the two groups of IDS: network-based and computer/host-based IDS [8]:

- Network-based IDS are used for monitoring and analysis of data packages, which are transferred through the network. A traditional sensory architecture monitors all network traffic, while the distributed architecture monitors a specific part of it, in a particular piece of equipment. The main purpose of the network-based IDS is protection from external attacks.
- Computer/host-based IDS use data for analysis, which origin from computer host journals, i.e. the data sources for the computer/host-based include event logs, application logs, etc.

The host-based IDS are efficient in identifying malicious actions on the network, as the data used for analysis are located on equipment used by authorized users. Event logs give information about events of access of files on the particular piece of equipment, i.e. the host-based IDS aim at identification and reaction to attacks by inside users, which is the difference between the two IDS realizations.

4.5. Methods and tools for protections from known threats

According to the ISO/IEC 27002 standard [9], the education in the field is completed by studying different methods and tools for protection from known threats. Here are listed the basic legal and administrative methods; organizational measures; technical, software, and specialized protection tools that should be discussed in IS courses.

The legal methods concern the legal basis used for solving the problems. Each organization has legally-based documents that address the organization's defenses.

Administrative methods – these are all decrees, regulations and rules regarding the information security in the organization. Also, there must be a person to be responsible for the information and personal data security.

The organizational measures can be of various types. For example, activities related to: the personnel recruitment and training; restricted access to the server room, where sensitive and classified information is stored; development of procedures on personal data security, etc.

The technical tools include locks, handles, bars, security alarm system, video surveillance, etc. The software protection is based primarily on identifiers and passwords. They are set up not only for operational systems, but also for applications, data base, etc.

Specialized protection tools can be realized as technical, software or hybrid tools. Such a tool is, for example, a computer anti-virus program; a firewall can be a specialized hardware tool, as well as a piece of software.

The student should understand a balance is needed between the value of the protected subject or resource and the cost of the protection system.

5. Working on projects in Information Security Courses

Working on projects has been widely embraced in many courses, especially in Computer science area [10],[11],[12]. Having presented the students with the main concepts in information security, described in Section 4, the learning process continues with team projects, where students apply the obtained theoretical knowledge. The following sections are dedicated to sample topics and tasks, given to the students, which they explore and defend in the form of projects during the seminars. Topics are selected to meet most standards' requirements and help with the analysis of learning outcomes based on standards.

Using passwords

One of the ways to improve security is to protect the passwords. Increasing the number of symbols in a password is not acceptable to most of the users, therefore the efforts are directed to achieving a maximum secrecy and easy memorizing. In order to achieve this, students have to research different approaches, including puzzles, fingerprint technology, sequence of frequency strings, etc. [13].

Researching on the content of the exchanged information

At the moment, the security systems usually do not investigate the content of the information which is exchanged by the network users. Most systems only identify the username and password. The implementation of a system which monitors the content in most general terms would give information about: what is the reason for a worker to download information at 3 a.m., which is something they normally do at 9 a.m. from their workplace. The systems which support content monitoring for increasing the security allow for observation based on statistics on the behavior of the users, the connections they make based on their interests, etc. [14]. Such examples are WikiLeaks and the service Google mail, which registers if the user is logging in it from an unknown device, and requires of the user to confirm via their mobile phone that the access is not unauthorized.

Personal data privacy and data security

The students are introduced to GDPR, which includes regulatory mechanisms for collecting, using, processing, storing and providing personal information. In this context, the students are given a task to investigate the requirements for protection of the personal data which the users exchange. This is related not only to the protection of the property assets, but also to the possible moral consequences for the individual [15]. It is established that it is relatively easy to steal information, especially if it is in electronic form, and the consequences may prove unpredictable. The focus is on the mechanisms of identification, authentication and authorization used in the software systems, including Grid security approaches and service-oriented applications [16]. Different traditional and personalized models of access control, based on attributes, roles, organization, etc., are presented [17], [18], [19], [20]. The classification of the attacks directed to data disclosure, provided in [21], is used.

Attacks on electronic articles and publications

There has been an increase in the information misuse in some of the electronic media. The increase in the number of articles in Wikipedia is exponential. This information flow cannot be monitored manually by the editors. The first tools to monitor the changes in the articles, which lead to distorted information were AntiVandlBot and VandalProff. AntiVandlBot is a simple set of rules, which allows monitoring on the changes in the articles and their automatic rejection. VandalProof uses a graphical user interface, written in Visual Basic, which allows to find editors who do not have the necessary confidence, and to reject the corrections they have made. In this case students have the task to look for new tools, which can allow faster editing and ways of agreeing with the Wikipedia article authors. Some features of such systems are described in [22].

Attacks on web applications

Here students investigate threats directed to web applications and to the information used by the users while taking certain actions on the web. One threat which continues to spread is cross-site scripting (XSS), whose main idea is to use a special character, which makes the web browser switch from data processing to code processing. For example, when an HTML page is initialized as data, the hacker can introduce a character (through Java script code), which provokes the Java Script interpreter. If the application does not filter such special symbols, the XSS intrusion is successful and can lead to using the user's account, or other user data or attributes.

Smart home security

While providing more home comfort, threats are generated by the remote access, managing different household appliances, and other intelligent sensors and systems. Threats arise, associated with the interaction between technologies and their users [23]. In these cases, students' research focuses on the impact on the communication channel using different protocols, and control of the overload due to denial of service attacks (DDoS).

Impact of the multimedia

The research on this element of the digital society is related to the need for users to get entertained and to exchange information using contemporary audiovisual media, including live interaction, which leads to a high degree of realistic presence. The integrated use of solutions like DES, AES, IPv6, MPEG2,4, DVB formats, etc. while transferring multimedia contents allows transformation of the multimedia into hypermedia [24]. This triggered a number of problems, related to the multimedia content, its protection, and its impact on the users. The addiction to hypermedia entertainment influences user's behavior in their everyday life, which in turn poses questions about their usefulness and about the control over them, especially for adolescents [25]. Another task posed to students is the problem with the copyright of hypermedia content, and its guarantee in the digital society requires a combination of legislation and technological solutions.

Social engineering

The students have the task to investigate the major existing threats connected to social engineering, directed to social manipulations, revolutions [26], and negative impact on adolescents [12]. When researching this issue, it is essential to note the following two aspects: the role of the marketing campaigns, which collect user data based on their habits, behavior, usage of different devices for access; the psychological attitudes and dynamics of the users in the social networks, which can be monitored and used both directly and indirectly [27].

Virtual environment threats

Many organizations install virtual operation systems, which allow several applications to work on a single server, thus decreasing the number of physical computers, which is economically viable. This approach is essential for the data centers, where thousands of servers are used. According to [28], industrial organizations have built up 80% virtual infrastructure on their servers. In case of attack of the host server, the layer of the OS responsible for the virtualization is compromised. This poses a threat to all virtual machines, respectively to data and applications they perform. Program security systems typically do not track the traffic between virtual machines and cannot register the attacks. This leads to serious cyber threats on service users. In addition, the virtualization process is dynamic − virtual engines are systematically created and switched off to different hosts. This requires a dynamic security system. Different protection tools exist, which are investigated by the students, such as virtual protection systems of HP, IBM, Juniper and McAfee, which work as applications within the operation system of the main computer.

6. Analysis of the training process and results

The training process, aiming at raising the awareness regarding different types of risks and threats for the information systems and networks related to meeting the information security standards and information protection, relies on the training method described above, and on its realization through project based learning.

After completing of each IS course, it was a subject to a thorough analysis. The analysis was based on:

- students' achievements;
- students' activity during lectures and seminars;
- student-lecturer interaction intensity;
- analysis of the results of training without using the standard;
- students' professional realization.

To this end, a quantitative analysis of the knowledge and skills acquired as a result of the training was performed. This analysis was based on the results from the final exam on the subject, the results of the formative assessment, and the results from the projects. The exams usually consisted of solving a test of 50 questions, related to the theory and application of the learning material.

The analysis of the results, as well as of the difficulties encountered during the training, confirmed all the positive expectations and envisioned difficulties, identified as a result of applying project based learning in other disciplines. Additional obstacles for information security training are the lack of adequate learning materials, adapted for the educational purposes, as well as the technical incapability for the training to be performed on different software platforms.

The professional realization of the students trained via the above described way confirmed our expectations that they perform better at both analytical and applied levels. Furthermore, as a result of these trainings, an improved relation with the business, state administration, and society is obtained. We also believe that this education will lead to increased level of information security in different areas.

In order to update and improve the curricula on information security, we intend to assess the computer competences (knowledge, skills and attitudes/proficiency levels), achieved as a result of the education, by using the methodology used in [29]. We also plan to develop a cloud application, which will support the lecturers in preparation and management of the projects; allow for control over the authorship of the projects, as well as the degree of participation of each of the team members in the group project; support the students in managing their own learning process. It is our plan also to design cloud structures and software approaches to support the education in the field.

7. Conclusions

The article presents an approach for education in the field of Information security, which is delivered in several Bulgarian universities. It is based on using standards, investigation of selected appropriate real-life problems, and analysis of different situations. This education supports the view of the article authors that the students in Computer Science & IT areas should constantly look for new approaches for problem solving and applying new technologies.

The limitation of threats in a digital society depends on the creation of rules, their observance and the development of a culture of behavior. It takes time and needs a strong technological support. At the end of 2018, a National Scientific Program "Information and communication technologies for united electronic market in the field of science, education and security" was launched in Bulgaria which in the authors' belief will lead to many positive results in the information security area.

Acknowledgements

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.

References

[1]. Humphreys, Ed. (2016). *Implementing the ISO/IEC 27001 ISMS Standard, Second Edition*, ISBN 13: 978-1-60807-930-8, ARTECH HOUSE.

[2]. ISO/IEC 27001: 2006. Information Technology. Security methods. Information security management systems. Requirements (ISO/IEC 27001:2005).

[3]. Pfleeger Ch., & Pfleeger, Sh. (2012). *Analyzing Computer Security. A Threat/Vulnerability/ Countermeasure Approach*, Prentice Hall, ISBN-13:978-0-13-278946-2, 799 pages.

[4]. Quality management systems, Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en (ISO 9001:2015). [accessed: 10 March 2019].

[5]. To The Point, Retrieved from: http://iso14001.guide/ [accessed: 17 February 2019].

[6]. Patias, I., & Ilieva, S. (2018). *Project Risk Management*, ISBN 9789540742625, published by University Press "St. Kliment Ohridski", Sofia, Bulgaria.

[7]. Petters J., Data Security, Retrieved from: https://www.varonis.com /blog/ids-vs-ips/ , [accessed: 10 March 2019]. [accessed: 15 March 2019].

[8]. Preetham. V. (2005). *Internet Security and Firewalls,* Premier Press 2002. 337 pages. ISBN: 1-931841-97-7.

[9]. ISO/IEC 27002:2005(E). Information technology – Security techniques – Code of practice for information security management.

[10]. Patias, I., (2018). Teaching Project Risk Management with a Positive Approach, *Journal of Engineering Research (AJER)*, *7*(2), 207-210.

[11]. Stefanova, E., Sendova, E., Deepen, N., Forcheri, P., Dodero, G., Miranowicz, M., & Brut, M. (2000). Innovative Teacher-Methodological Handbook on ICT-enhanced skills., 2000, Sofia.

[12]. Todorova, M., & Orozova, D. (2016). How to Build up Contemporary Computer Science Specialists – Formal Methods of Verification and Synthesis of Programs in Introduction Courses on Programming, Proceedings of 9-th Annual International Conference of Education, Research and Innovation, Seville, 14th, 15th and 16th of November, ISBN: 978-84-617-5895-1, 4249-4256.

[13]. Bianchi, A., Oakley, I., & Kwon, D. S. (2012). Open sesame: Design guidelines for invisible passwords. *Computer*, *45*(4), 58-65.

[14]. Global Risks Report, (2012). Seventh Edition, World Economic Forum. Retrieved from: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf. [accessed: 12 January 2019].

[15]. Gaff, B., Loren, R. & Spinney, E. (2012). Intellectual Property, Part Il − Computer, IEEE Computer Society Publ., February 2012b, 9-11.

[16]. Goranova R., (2008). Security in Service-oriented Grid, AIP Conference Proceedings, AMEE'34, Volume:1067, American Institute of Physics, .541-548, ISBN:978-0-7354-0598-1.

[17]. Inter National Committee for Information Technology Standards, INCITS 359-2012. (2012). Information Technology – Role Based Access Control, Retrieved from: http://www.techstreet.com/standards/incits-359-2012?product_id=1837530. [accessed: 05 January 2019].

[18]. National Institute of Standards and Technology. (2014). Guide to Attribute-based access control (ABAC) Definition and Considerations, Retrieved from: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf. [accessed: 06 January 2019].

[19]. Zhang, Z., Zhang, X., & Sandhu, R. (2008). Handbook of Research on Social and Organizational Liabilities in Information Security, In Chapter 6: Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration, ISBN: 1605661325, 94-117.

[20]. Hadzhikolev, E., Hadzhikoleva, S., & Andonov, N. (2018). Challenges in Creating University Digital Document Repositories. *Compusoft*, *7*(11), 2846-2851.

[21]. Dimitrov, V., (2017). Attacks based on information disclosure, Proc. of International Scientific Conference “The Problems of Applied Mathematics and Computer Science”, Aktobe, Kazakhstan, 262-264, ISBN: 9789965074202.

[22]. Halfaker, A., & Riedl, J. (2012). Bots and cyborgs: Wikipedia's immune system. *Computer*, *45*(3), 79-82.

[23]. Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., ... & Scholl, H. J. (2012, January). Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

[24]. Balzarotti, D. (2012). *D4. 2: Second Report on Threats on the Future Internet and Research Roadmap*. Technical report, SySSeC Consortia.

[25]. Bavelier, D., Green, C. S., Han, D. H., Renshaw, P. F., Merzenich, M. M., & Gentile, D. A. (2011). Brains on video games. *Nature reviews neuroscience*, *12*(12), 763-768.

[26]. Ghannam, J. (2011). Social Media in the Arab World: Leading up to the Uprisings of 2011. *Center for international media assistance*, *3*(1), 1-44.

[27]. Buckland, B. S., Schreier, F., Winkler, T. H., & Centre pour le contrôle démocratique des forces armées (Genève). (2010). *Democratic governance challenges of cyber security*. DCAF.

[28]. Garber, L. (2012). The challenges of securing the virtualized environment. *Computer*, *45*(1), 17-20.

[29]. Sharkov, G., Asenova, P., Ivanova, V., Gueorguiev, I., & Varbanov, P. (2014, July). Evaluation of ICT Curricula Using European e-Competence Framework. In *Proceedings of: 10th Annual International Conference on Computer Science and Education in Computer Science* (pp. 4-7).