BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2023 • Vol. **79**, pp. 55-66
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.79.23.03

Some Aspects of Information Security and Cybersecurity Problem Area

Ivan Gaidarski[1], Pavlin Kutinchev[2]

[1] Institute of Robotics (Unmanned Robotic Systems Lab),
Bulgarian Academy of Science, Sofia, Bulgaria
[2] Institute of Information and Communication Technologies,
Bulgarian Academy of Science, Sofia, Bulgaria
Emails: ivangaidarski@ir.bas.bg, p.kutinchev@gmail.com

Abstract: Design and development of Information Security System (ISS) is complex process. The developer of ISS must have all needed information about the requirements, which is defined in Problem Area. One approach is to perform an analysis from different perspectives of the interested parties, which give a complex picture of the problem area. Through a risk analysis, the system developers can select the necessary operations and activities so that the tasks in front of the ISS are fulfilled. An analysis of the problem area is done, with focus to two viewpoints – Information and Cybersecurity. It is important to make some clarifications and find common and different aspects between them. This is done with the help of some basic concepts and their relations, of the both cybersecurity and information security domain – vulnerability, threats, threat actors, threat vectors and attacks. An analysis to both attacks and Approaches to protection (AP), which are protection measures in the form of actions, processes or procedures taken to protect an information system from attacks on the Confidentiality, Integrity and Availability of the ISS is done.

Keywords: Information, Cyber, security, system, development, analysis, aspects, viewpoints, vulnerability, threat, attack, protection

1. Introduction

The systems development cycle shown in Fig.1 is used to design an information security system (ISS). It consists of several main components and connections between them:

- *Problem* – Implementation of a certain way of functioning of the ISS, which must work in a given environment.

- *Problem area* – defines the area in which the problem is solved.
- *Implementation environment* – represents the conditions under which the ISS is implemented.
- *Stages* – The stages through which the development of the ISS must go.
- *Creation of ISS models* at different stages of the development.
- *Transforming of models* from one type to another.

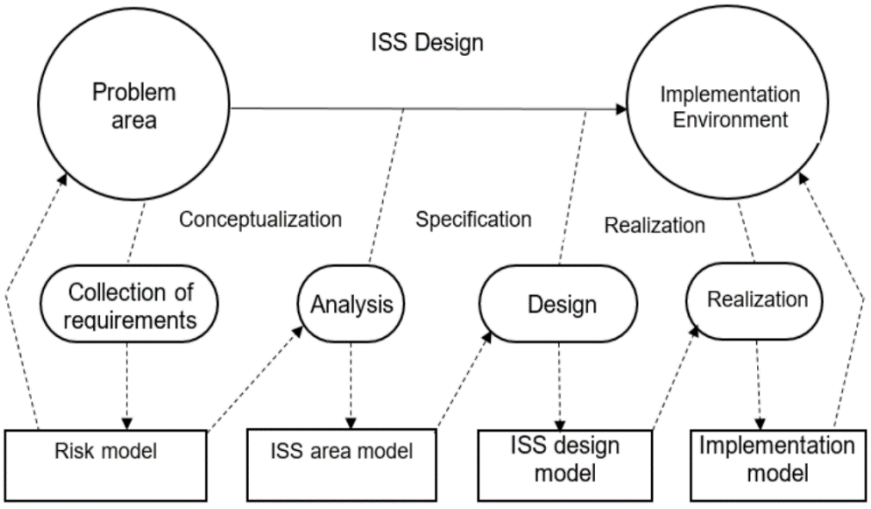

Fig. 1. Systems development cycle

The problem area defines the requirements toward ISS. Due to their complex nature, it is necessary to assess which of them should be met by the ISS in the context of effort, technical means, human resources and cost. This is done through a risk analysis.

The process of ISS development passes through the following stages:

1. *Collection of requirements* – In this stage, the identification of the requirements and, accordingly, the possible risks to the system is carried out. In this way, system developers get the necessary information about what effort and resources it will cost them to solve the problem from the point of view of individual users.
2. *Analysis* – study of the problem area from the different perspectives of the interested parties.
3. *Design* – design of the architecture and processes in ISS;
4. *Realization* – carrying out the specific implementation of the ISS in a given environment.

Different models are created at separate stages of development. They are created by transforming a model from one type to another:

- Based on the collected requirements for the system, a Risk Model is created to describe the risk, which is managed by the ISS,
- As a result of the analysis of the problem area, an ISS area model is constructed.
- Description of the architecture and functionality is done using the ISS Design Model
- Depending on the conditions under which the designed ISS will work, an Implementation Model is constructed.

Every organization in its daily activities performs various operations with data in its information environment. This also sets serious requirements for the protection of these information resources. Individual users in the organization perform different activities on data processing and operations with them, which contributes to the complexity of the requirements for ISS. Adding the fact that different types of data are processed, used and communicated (Data in motion, Data in Use and Data at rest) it only complicates the task of the ISS. Due to the above arguments, the design of ISS is a complex task in which many specialists take part – the so-called interested parties. These are lawyers, specialists in compliance with various standards and best practices, system architects, developers, testers, support specialists, etc. Each of them has a certain sphere of competence, defining specific requirements for the system. The analysis of the different points of view of the interested parties to an ISS enables the developers of the system to combine their requirements so that the tasks set before it is fulfilled.

In this article, we consider some aspects of problem domain analysis. This analysis is carried out from different perspectives of the interested parties and gives a complex picture of the requirements for ISS. We look at Information Security and Cybersecurity perspectives and the differences between them.

2. Information security and Cybersecurity

Cyberspace, Information Security and Cybersecurity.

According to the National Cybersecurity Strategy "Cyber Resilient Bulgaria 2020" [1] Cyberspace is the electronic or "virtual" world of interconnected communication and information systems, in whose networks the global community of over 3 billion citizens, or more than 45% of the earth's population exchange information, ideas, services, business and friendship, without territories and borders. Cyberspace is an interactive environment of electronic networks and information infrastructure used to create, destroy, store, process, exchange information, manage objects, systems and services [2]. Another definition from the same source says that the field in which the information environment composed of independent networks of information system infrastructures

including the Internet, telecommunications networks, computer systems, embedded processors and controllers are used to process, store and transfer information and user activities. According to the Law on Cybersecurity of the Republic of Bulgaria, Cybersecurity is a state of society and the state, in which, by applying a complex of measures and actions, cyberspace is protected from threats related to its independent networks and information infrastructure or that may disrupt their work [3]. According to the same sources, cybersecurity includes network and information security, countering cybercrime and cyber-defense.

Cybersecurity is a state of cyberspace determined by the level of confidentiality, integrity, availability, authentication and fault tolerance of information resources, systems and services. It is based on the effective construction and maintenance of proactive and preventive measures [1, 2].

Definitions of information and cybersecurity vary according to different sources and different perspectives. Therefore, it is important to make some clarifications and find the common and different aspects. Apart from interconnected communication and information systems (hardware) processing and communicating data, an important element of cyberspace are people. Each of the concept systems, data and people (see Fig. 2) has its role and interrelationship with the others and determines the processes taking place in cyberspace and their dynamics.

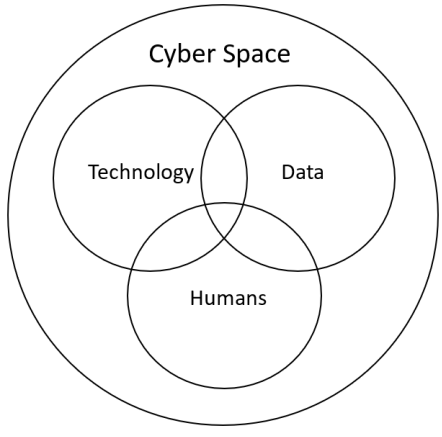

Fig. 2. Components of Cyberspace

At the same time, each of the components affects the rest and the cyberspace as a whole [4]. The different concepts enable a view to cyberspace from different perspectives.

Data Perspective looks at electronic data in its various forms and states. Such states, for example, are the three main types of data - Data in Motion, Data in Use and Data in Rest (Fig. 3).

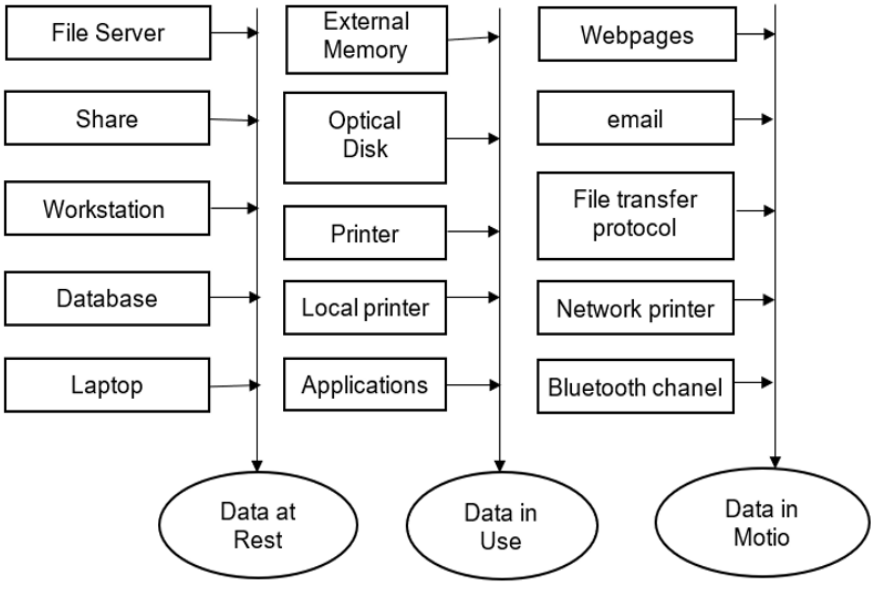

Fig. 3. Data types

At Data in Motion, we have data that is communicated and transported, for example, data inside hardware systems, communication between them, communication with external systems and communication with people. Data in Use is the data that is processed by the hardware systems and is used by them and people. Data at Rest is the static data stored in storage devices for the purpose of archiving, standing on disk shares or simply in a directory in the local workstation that is not in use.

Technology Perspective looks at the connected systems in cyberspace, along with the data that is transported, processed, used or archived. This includes computing hardware, software - operating systems, servers and applications.

Cybernetic Perspective considers the presence of people in cyberspace as an active part of the dynamics of the environment. People use communication and computing systems, create, use and communicate data. In practice, people are the most important part of the *ecosystem* because they are the creators and consumers of the information resulting from the work of the other components.

As seen from the different perspectives, the three components of cyberspace partially overlap with each other due to their interdependence.

Information security and cybersecurity are not static either. They are dynamic concepts that overlap to some degree, with individual components changing over time, entering the space of the other concept, or being present in both at the same time. According the National Institute of Standards and

Technology (NIST), information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability, while cybersecurity is the ability to protect or defend the use of cyberspace from cyber-attacks [5]. Information security is related to the concepts of confidentiality, integrity, and availability, or so called "CIA Triad":

Confidentiality – refers to the confidentiality of data and systems, the prevention of disclosure or access to information by persons without the relevant authorization. In organizations dealing with large amounts of information, data can be classified with different levels of security, according to the current regulatory framework and internal criteria. Ensuring confidentiality requires that all persons with access to sensitive information understand the involved risks and take appropriate responsibility in handling that information.

Integrity – defines the assurance that information in the organization has not been altered, added or deleted without the appropriate permission. Common measures to protect integrity include encryption of data at rest and hashing of data in motion, file access rights, version control to prevent accidental modification or deletion.

Availability – this concept guarantees availability and accessibility of data and systems whenever they are needed. For this purpose, various technologies are used, providing fault tolerance, load balancing, redundancy of hardware and software components and various procedures, such as backup and disaster recovery plans.

To address the differences and commonalities between Information security and cybersecurity, we examine them in the context of their various definitions. For example, the focus of cybersecurity is on measures and actions taken to prevent unauthorized access, alteration or destruction of cyber resources and data. Both of the concepts assess potential risks, including determining which data is relevant, methods, policies, procedures and technologies to protect cyberspace [4]. Here are some aspects in which Information security and cybersecurity differ or overlap:

Digital and non-digital assets. Both Information Security and Cybersecurity address threats to digital systems and data. Typical examples are DoS and Ransomware attacks and the corresponding approaches to protection (AP). The difference is that while cybersecurity covers only digital systems and data, information security also includes non-digital forms of data storage such as physical documents.

Human and Non-Human Threats. Another aspect where the two concepts overlap are human threats. While cybersecurity is mainly focused on human threats, where attacks are carried out by people, information security must also

consider various non-human threats, such as fire protection in a room where physical documents are stored.

Data vs. Everything Else. In this aspect, the overlap between cybersecurity and information security is their focus on protecting the organization's data. While information security is entirely focused on data protection, cybersecurity covers other threats to an organization's IT assets, such as securing the functioning and access to web applications.

3. Analysis of Cybersecurity/Information security domain

Some of the basic concepts and their relations, of cybersecurity and information security domain are shown on Fig. 4.

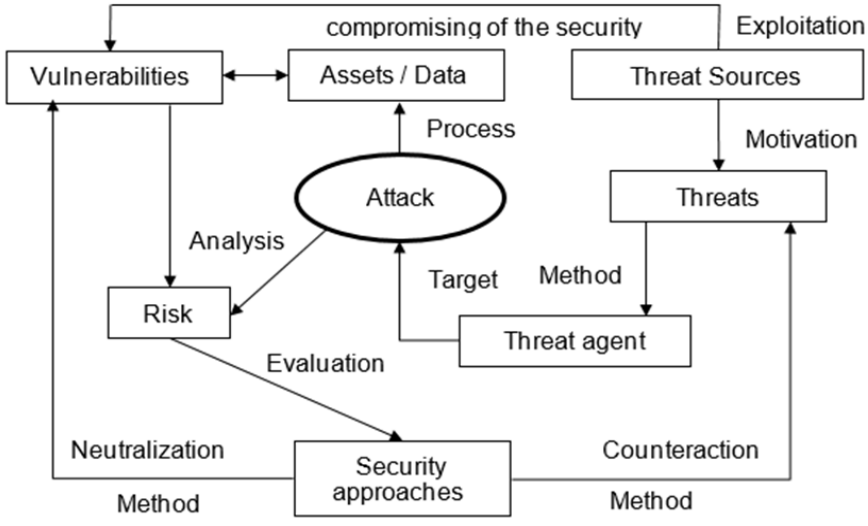

Fig. 4. Vulnerabilities, threats and attacks

Vulnerabilities are weaknesses that a threat source exploit to conduct a successful attack on information assets. *Threat* is the ability of the threat source to exploit a specific vulnerability, resulting in a security breach [6, 7, 8].

According to the threat vector, threats can be classified into internal and external. Due to the nature of the threat to electronic assets and data, external threats are characteristic of both domains – cybersecurity and information security. Internal threats can be to both electronic and physical assets and data, so they are characteristic of Information security.

External threats. The vector of the attack of external threats is "outside – in", against the protected information assets. External threats use the principle of the weakest link. The attacking party tries to find security vulnerabilities through

which it can penetrate the secure network and take control of the assets. Examples here are: Hacker Attacks, DoS Attacks, Worms, Trojans, Botnet, DoS and DDoS Attacks, Drive-by Exploits, Code Injection Attacks [7].

Internal threats. An incident caused by an internal threat occurs when an insider – employee, partner or third-party provider with authorized access to sensitive information, intentionally or accidentally misuses this access, leading to negative consequences for the organization. There are many causes for incidents involving internal threats: careless behavior of the insiders, suppliers and external contractors, too strict cybersecurity policies, leading to Security Fatigue, theft of electronic identity and malicious users. Internal threats can be divided into several main groups according to their source: Human Threat, User Activity, and Business Applications.

When a threat source takes intentional action to compromise the security of asset by disclosing, altering, stealing or destroying it, by exploiting a specific vulnerability we have an *Attack*. In order to neutralize the attack, it is necessary to perform an analysis of the conditions it depends on - vulnerabilities of assets in various working environments, threats, sources of threats, threat agents and their motivation [8, 11]. It is also essential to know how different types of attacks work, the risk they pose to assets, and the appropriate security approaches that can be used as countermeasures for protection [9, 10, 11, 12, 17, 18].

The different types of attacks can be categorized into several categories: Interception, Interruption, Modification and Forgery. Each category may touch on one or more of the concepts of the "CIA Triad" (Fig. 5).

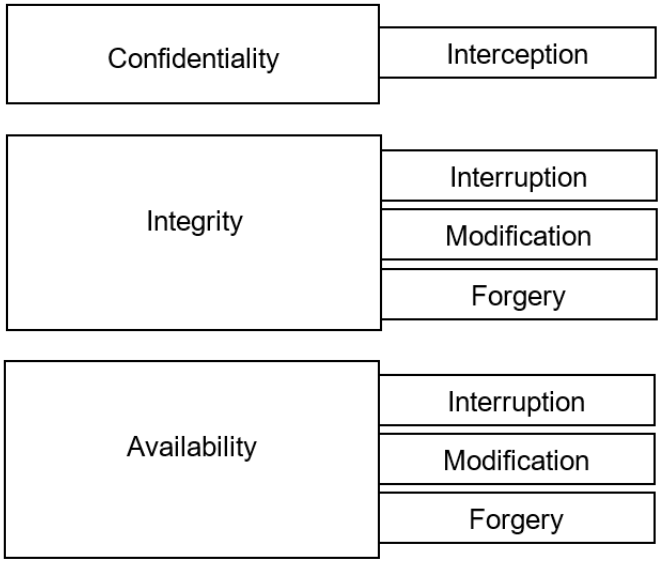

Fig. 5. Types of attacks

Interception. These types of attacks allow unauthorized users to access data or information assets. They are essentially attacking Confidentiality as element of "CIA Triad". Interception can take the form of unauthorized viewing or copying of files, wiretapping of telephone conversations or unauthorized reading of e-mails. They can act against "Data at Rest" and "Data in Motion". This type of attacks are characteristic of both the Cybersecurity domain and the Information Security domain.

Interruption. These attacks lead to temporary or permanent unusability or unavailability of data or systems. They concern both Availability and Integrity from "CIA Triad". For example, a DoS attack on a mail server can be given – which is attack on Availability. In the case of a database manipulation attack, we have an attack on Integrity because of the possible loss or corruption of data. This attack can also be categorized as Modification if the result is data alteration. The *Interruption* type of attacks are characteristic of both domains – cybersecurity and information security.

Modification. The typical Modification attack is tampering of data or information assets. These attacks target both the Integrity and Availability category. An example can be unauthorized access to files and alteration of the data it contains. This is attack on Integrity. If the affected file is for example system configuration file, the way the system works can be changed. The result will be corresponding services to be affected (for example Web server), which will be attack on its Availability. If the modification of the file also changes the way the system serves e.g. encrypted connections, it will impact the Confidentiality. These types of attack are characteristic of both the cybersecurity domain and the information security domain.

Forgery. Attacks of this type involve the unauthorized generation of data, processes, communication or other activities through a given system. These attacks primarily affect Integrity, but can also be considered Availability attacks. Examples of such an attack include generation of false information in a database, sending forged e-mail on behalf of the authorized user, which is commonly used as a method of spreading malware, and spear-fishing attacks. An attack of this type can also be an Availability attack, if the attacker manages to generate enough processes consuming system resources (e.g. Network or Web traffic). It can cause overloading of the system, with result crashing and becoming unavailable to legitimate users. These types of attacks are also characteristic of both domains – cybersecurity and information security.

Approaches to protection (AP) are protection measures in the form of actions, processes or procedures taken to protect an information system from attacks on the confidentiality, integrity and availability of the information system. The goal is to reduce the risk associated with information security [14]. According

to the time of their action, AP can be logically grouped into several categories as shown in Table 1 [13, 14, 15]:

Table 1. Implementation of AP

AP	Base	Cyber-security	Information Security	Examples
Physical security AP	Real world	--	Yes	Locks, Safes, Alarm systems, Portals, Doors, Fences, Warning signs, etc.
Administra-tive AP	Current legislation, regulations, standards and good practices	Yes	Yes	Information security policy, data protection policy, accepted access rules, fines and administrative penalties, etc.
Techno-logical AP	Computing and communication devices, software systems	Yes	Yes	Video cameras, Firewalls, IDS/IPS, Access control, SIEM, Backup, DLP, Malware protection and more.
Operational AP	Human factor	Yes	Yes	Security, IT security employees, employees who have passed Security Awareness trainings, etc.
Virtual AP	Software tools working with other AP	Yes	Yes	Access Control Lists, IP Address Lists, Password Policy, 2FA Authorization, Geolocation

- *Preventive* – Block threats before they take advantage of a given vulnerability.
- *Disclosure* – Detect and warn of attacks in real time, at the moment of their occurrence.
- *Deterrent* – Prevent external attacks and violations of the adopted information security policies.
- *Corrective* – Restore the integrity of data or other affected assets.
- *Restorative* – Restore the availability of attacked and disrupted services.
- *Compensatory* – Compensate the consequences of successful attacks against given security controls through one or more of the remaining unaffected controls. They are used in a multi-layered security strategy.

The main difference between information security and cybersecurity is the data being protected. While cybersecurity primarily deals with data in electronic format, Information Security encompasses data in all possible forms – electronic, physical (written) and intellectual. For this purpose, in addition to measures for

the protection of electronic data, measures such as physical protection of physical documents, provision of physical levels of access, etc. are also included.

Approaches to protection can have a different implementation as shown in Table 1 [12,13,14]:

- Physical security AP – physically present in the real world.
- Administrative AP – are defined and applied by the management based on the current legislation, regulations, standards and good practices;
- Technological AP – performed by computing machines;
- Operational AP – performed by people;
- Virtual AP – they are activated dynamically, when certain circumstances arise.

4. Conclusion

In the process of design of information security system, one of basic steps is to define the problem area, which is the area in which the system main problem is solved. As it defines the requirements toward the ISS, the developer of the system must have all needed information. The best approach is to carry an analysis from different perspectives of the interested parties, which give a complex picture of the requirements for ISS. Through a risk analysis, the system developers have the opportunity to select the necessary operations and activities of the various architectural elements of the system, so that the tasks in front of the ISS are fulfilled and at the same time the requirements regarding the deadlines, the budget and the necessary resources are met.

Acknowledgement

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement No. Д01-74/19.05.2022.

References

1. Национална стратегия за киберсигурност „Кибер устойчива България 2020”, Юли 2016, http://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120, last accessed 2023/05/17.
2. Maurer, T., Morgus, R.: Compilation of existing cybersecurity and information security related definitions federal department of foreign affairs. Switzerland, (2014).
3. Закон за киберсигурност, приет на 31 октомври 2018, 7 ноември 2018, https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf, last accessed 2023/05/17.
4. Edgar T., Manz D.: Research Methods for Cyber Security, Elsevier Inc. 2017.

5. NIST Special Publication 800-30 Information Security, Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, last accessed 2023/05/17.
6. Suryateja, P.S.: Threats and vulnerabilities of cloud computing: A review. International Journal of Computer Sciences and Engineering, Vol. 6(3), (2018).
7. The European Network and Information Security Agency (ENISA) (2012), https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2023/05/17.
8. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 rev.1, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, last accessed 2023/05/17.
9. ENISA Threat Landscape Report 2020 - 15 Top Cyberthreats and Trends, European Network and Information Security Agency (ENISA), 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed 2023/05/17.
10. Andress, J.: The basics of information security: understanding the fundamentals of InfoSec in theory and practice, Elsevier Inc. (2011).
11. Taylor-Duncan, L.: Come in, we're open – Keeping your company's IT data safe from threats, Techni-Core productions, (2014).
12. Chehlarova, N., Tsochev, G., Kotseva, M., Miltchev, R.: Digital competencies of public administration employees related to cybersecurity. In: 12th National Conference with International Participation (ELECTRONICA), 1-4, (2021) doi: 10.1109/ELECTRONICA52725.2021.9513705.
13. Rhodes-Ousley, M.: Information Security the Complete Reference. In: 2nd Edition, The McGraw-Hill, (2013).
14. Keung, Y.: Information Security Controls. Advances in Robotics & Automation 2013, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong.
15. Bhaskar, S.M., Ahson, S.I.: Information security: A practical approach, Oxford: Alpha Science International Ltd. (2008).
16. Schweitzer, J.A.: Managing information security: Administrative, electronics, and legal measures to protect business information. Boston: Butterworths. (1990).
17. Madzharov, A. N.: Technical implementation of a reporting system and its workflows. In: Proc. of International Scientific Conference "Defense Technologies" DefTech (2019), 01-03.10.2019. Shumen: Nat. Military Univ. "Vasil Levski", Faculty of Artillery. pp. 316-322.
18. Tianxing, M., Yoshinov, R., Osipov, V., Zhukova, N., Schukina, M., Evnevich, E.: Problems of human secure interaction with the Internet space. Problems of Engineering Cybernetics and Robotics, 75, 15-34, (2021), https://doi.org/10.7546/PECR.75.21.03.