Годишник Телекомуникации 2019, том 6, с. 37-44

Yearbook Telecommunications 2019, vol. 6, p. 37-44

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.4

TRENDS IN THE USE OF HIGH TECHNOLOGY SOLUTIONS FOR CYBERSECURITYOF CRITICAL INFRASTRUCTURE

Yoana Ivanova

Abstract: The aim of the paper is to present innovative technologies that contribute to strengthening cybersecurity of critical infrastructure. It focuses on trends in the use of high-tech solutions for cybersecurity of critical infrastructure. They are analyzed the capabilities of the next-generation cybersecurity model, as well as the role of the simulation modelling and expert systems in the process of identifying and preventing cyber attacks.

The main result of the study is the description of the overall sequence of steps to be completed in a model in order to a simulation study of the impact of a DoS – attack to it. The applied conributions are expressed in developing the algorithms in the form of block diagrams because of the comparative clarity and accessibility of this approach. Therefore, they are suitable for implementation in professional simulation environments. The types of algorithms and their properties, as well as the symbolism of the geometric blocks used are explained in detail and supported by examples of author's empirical studies conducted in the selected simulation products.

Keywords: algorithm, critical infrastructure, cyber attack, cybersecurity, expert systems, machine learning, neural networks, simulation modeling.

1. INTRODUCTION

The term *„infrastructure“* (from lat. *"infra"* - foundation, *"structure"* - construction, location, interaction) gains citizenship during the Second World War when it is used primarily in logistics to designate all fixed and stationary installations, as well as means of securing and controlling the armed forces [1]. Originally, the term was introduced in the XIXth century by the Swiss officer and General Antoine-Henri, Baron Jomini, who is famous for being a remarkable military strategist. Gradually, the concept starts to be used in the area of computer science and security and etc.

According to the Law on Crisis Management (Crisis Management Act) *„critical infrastructure*” is a system of facilities, services and information systems whose disruption, malfunctioning or destruction would have a negative impact on the health and safety of the population, the environment, the national economy or the effective functioning of government [2].

In Bulgaria, critical infrastructure is subdivided into nine sectors, including *Telecommunication and Information Technologies, Energy, Transport System, Financial System, Cultural Heritage*. Critical infrastructure, and in particular its sectors, are the backbone of the country and society. Therefore, measures to strengthen and maintain a secure, operational and sustainable critical infrastructure are of paramount importance to national security.

In practice, in assessing and analyzing the sustainability of complex systems like sectors of critical infrastructure, their most important quality is the capability to adapt to the potential risks in the environment and in case of an adverse event, restoring normal functioning for a short period of time. This capability is defined by the term *"resilience"*. In the context of critical infrastructure, all tangible and intangible assets included in it are exposed to the continuous impact of various external factors, which is a test of its sustainability. If these influences can be determined as threats or not depends on whether they could have a negative impact on the system by obstruction of its normal functioning.

Consequently, the dependence between the system’s resilience to various physical and cyber threats and the system vulnerability is inversely proportional. Regular testing of the technical means of protection enables the timely detection of existing vulnerabilities in a system to assess the system vulnerability and the probable risk of undesirable consequences when system stability is low.

Although the social networks are the main source of cyber threats the limited use of Internet services and applications would not be an optimal solution to cybersecurity issues, because of the needs of modern society of communication and access to information resources. Cyber threats can cause not only identity theft, but also adverse events in physical reality affecting key components of sectors of critical infrastructure such as its specialized management systems.

2. TECHNOLOGICAL ASPECTS OF CYBERSECURITY

The technological aspects of cybersecurity are related to the implementation of effective methods and tools to prevent cyber attacks in order to avoid negative consequences [3, 4]. The timely identification of threats must be possible even in case that the protective mechanisms are overcome from the attacker.

The tasks to be performed are as follows:

- At the system level: by a correct configuration.
- At the data level: through access control mechanisms using means of identification and authentication.
- At the user level: receiving security breach information.

There are many methods for examining security issues (expert evaluation method, scenario method, workshop method, brainstorming and etc.). The commonality between them is that they are based on the gathering of expert opinions from the participants, but they differ in the mechanism of conducting the study (free discussion, anonymous, etc.)

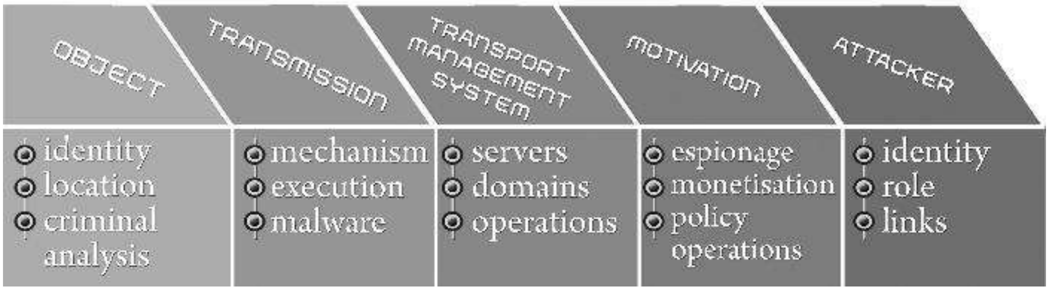
These methods support making conclusions about:

- The severity of cyber threats.
- The effectiveness of the technological means of prevention and protection.
- The need for implementing high-tech solutions and conducting research to strengthen cybersecurity.

Actually, the expert evaluation method is one of the most often used, because it is reliable and fast at the same time. This method includes the following stages:

- First stage: asking a question.
- Second stage: generating responses for a certain time.
- Third stage: processing the results.
- Fourth stage:a graphical representation of the results.

For example, if the question is related to the main phases of a cyber attack on TMS (Transport Management System), then the expert opinions could help for drawing a scheme as it is shown in Fig. 1.



OBJECT	TRANSMISSION	TRANSPORT MANAGEMENT SYSTEM	MOTIVATION	ATTACKER
identity location criminal analysis	mechanism execution malware	servers domains operations	espionage monetisation policy operations	identity role links

Fig. 1.Phases of a cyber attack to TMS.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.19.6.4

The steps to strengthen the cybercrime resilience according to an information document of the European Commission from 2018 are:

- The effective implementation of the first EU cybersecurity act (the NIS Directive - Directive on security of network and information systems) – this can be achieved by improving the cybersecurity capabilities of the Member States, international cooperation and risk prevention.
- The cooperation with the Member States – it is recommended strengthening ENISA (European Union Agency for Cybersecurity); building a European framework for certification, that can ensure the security of products and services in cyberspace; ensuring a rapid and coordinated response to large-scale cyber attacks.

The expectations are related to improving the coordination of work, access to expert knowledge, experimental research facilities and innovative cybersecurity solutions [5].

3. NEXT-GENERATION CYBERSECURITY MODEL

In this section is proposed a variant of next-generation cybersecurity model that could support the countering modern cyber threats (Fig. 2). The main components of this model are described as follows:

- Simulation modelling – in particular the agent-based modelling because of its main advantages like: an opportunity to create interactive simulations in which the user can influence the algorithm in real time; the models are very detailed; the results are reliable if correct data are entered as input parameters; the reducing financial costs. Agents themselves can be static or dynamic objects that have the ability to make decisions as well as interact with each other.

In a study of complex systems like critical infrastructures, it is necessary the system to be presented as a set of subsystems that are composed of components called assets. Subsystems and assets can be modeled as agents like vehicles, management structures, organizations, and etc.

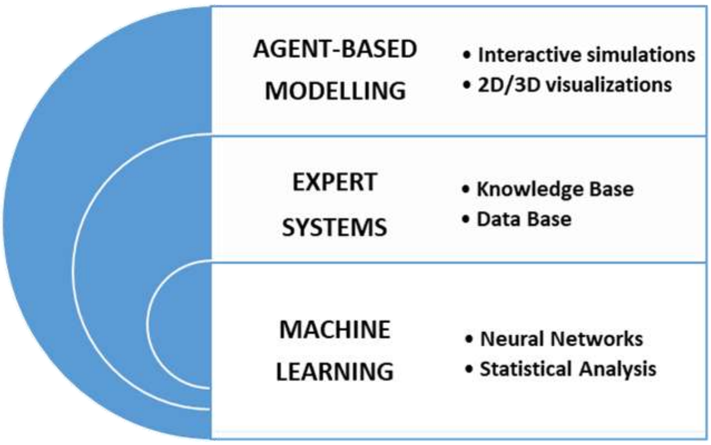


Fig. 2. Conceptual next-generation cybersecurity model.

- Expert Systems (ES) – they are characterized by AI (Artificial Intelligence) in management.

The notion of agent, which has already been explained in the context of agent-based modelling, is also widely used in the field of artificial intelligence. It is defined as something that perceives the environment through sensors and influences it through effectors that are a type of executive bodies [6].

An object of the field of AI is the design of agents whose impact on the environment or an interaction with it results in gathering knowledge about it. It is accepted that such agents are called *intelligent* because of their ability to communicate, perceive, and execute.

The main components of ES are data bases and knowledge bases. A large amount of information and especially multimedia can be stored in them. They are designed to solve problems of a different nature by using probability networks that function on the *fuzzy logic* created by Lotfi Asker Zadeh in 1973.

Fuzzy Logic is based on probability distribution for realization of an event. In the area of cybersecurity a cyber attack is such an adverse event. ES make logical conclusions by using Boolean operations - logical „and“, „or“ and „not“, based on expert (human) knowledge, which is represented by production rules.

Probability networks can be found in bibliographic sources under one of the following names: probabilistic networks, belief networks, Bayesian networks, causal networks, knowledge maps. In a conceptual sense, each network is built up of nodes and links between them. In a probability network, the nodes are composed of a set of random variables, and each node pair is linked by directed links or arrows. The intuitive meaning of an arrow from node X to node Y is that X has a direct influence on Y. Each node has a probability table that quantifies the effects of the parent nodes on it. Parental are all those nodes whose arrows are directed to the selected node and affect it [7].

- Machine Learning (ML) – it builds on AI because it is based on artificial neural networks that function in a similar way to the human brain. They represent realistic mathematical models of brain structures that are designed to process data by simulating the brain activity.

Actually, the name of this type of networks is not related to their technical structure but is due to their functionality. Although their components are bipolar transistors (semiconductor crystals with two p-n junction), their properties are analogous to those of biological neuronal systems that consist of nerve cells (neurons) and connective channels (synapses).

Each neuron has a cell body (soma) in which the cell nucleus is located. A long fiber (axon) and several shorter fibers (dendrites) exit from the soma. The contact with other neurons, muscles or glands is accomplished by the synapses [8]. As a result of this complex physicochemical process, the electrical potential in the body of the cell that receives the signal generated by the axon increases or decreases. When the potential reaches a threshold value, the neuron passes into an active state and the axon sends an impulse with a certain force and duration. After that there is a state of rest.

The main advantage of using neural networks is the ability that they add to AI - self-learning by self-modification. For example, they can be categorized as sources of cyber threats because of the capabilities of networks to detect and analyze features, interdependencies, and regularity in data streams.

These networks can be modeled, simulated and analyzed using specialized software. A suitable product for this purpose is SIMBRAIN [9] for designing multilayer perceptron networks. The workspace of SIMBRAIN contains components of the simulation, mechanisms for their connection to each other, and ready-made models that can be modified by adding neurons or synapses between them.

Initially perceptrons were explored by Frank Rosenblatt in 1960. In the perceptrons the inputs first pass through "preprocessors", which are called *associative units*. Their working principle is based on the associative memory, allowing different patterns to be associated with each other, if similar signs are available. In fact, the image recognition is one of a variety of advanced applications of this type of network.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.19.6.4

4. APPLICATION OF SIMULATION MODELLING IN STUDY OF THE IMPACT OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURES

This section of the paper is related to the algorithmization of the main steps in the process of modelling and simulation - from inputting data into the simulation models to generating output data and conducting assessment and analysis of them.

Enhancing cybersecurity is needed because the attackers use new approaches for a breakthrough in the system. The SQL injection and Cross-site scripting (XSS) are two of the most often software and protocol vulnerabilities in web applications that should be detected in a timely manner. Cybersecurity policies are based on advanced methods for vulnerability assessment and analysis. Preliminary tests in a simulation environment help preventing cyber attacks and building effective protections.

Actually, the working principles of simulation systems are based on a probability distribution of random variables. The software products can be classified depending on their ability to support solving problems in various fields. The basic algorithms for modelling random variables include two consecutive main actions of generating values of random variables and calculation of the results. The condition is related to the sufficiency of the simulations results. This means that if their number is insufficient, then it is required more values to be generated. A cyber attack is a random event. Therefore, its random realization is every attempt for answering the following questions:

- If the cyber attack C has been realized?
- Which cyber attack (Ci) has been realized in case that a few types of cyber attacks are possible (C1, C2, …Cn)? –for example, it could be APT (Advanced Persistent Threat), DoS (Denial-of-Service), DDoS (Distributed Denial-of-Service) and etc.
- What is the value of the studied random variable?
- What is the set of values of the system of random variables? [10]

The main characteristics of algorithms are determination and efficiency. It means that they must contain accurate and clearly described rules on the one hand and to ensure obtaining one or more results in the execution of the sequence of instructions on the other hand.

The method of presenting the simulation process by block diagrams is a good practice in the area of simulation modelling used and established by experts in that field [11]. The main advantages of this type of algorithmization are its clarity and the possibility the block diagrams to be easy edited or to be expanded according the specific aims.

Depending on the way they are structured the block diagrams are linear, branched, cyclic or combined and may contain the following basic blocks: start/ end/ pause (in an oval); action (in a rectangle); input/ output (in a parallelogram); condition (in a rhombus) and etc. Actually, a sequence of steps could be presented by more than one block diagram. One of the essential differences between the linear and branched block diagrams is the analysis block which is not available in the linear schemes.

In this paper the algorithms are presented graphically in the form of exemplary block diagrams. The correctness of algorithms needs to be verified by satisfactory result which can be machine - or human-generated data from empirical research in a simulation or a physical environment. The most important goal that should be achieved is the conviction and security of the potential users of the algorithm that it “correctly takes all instances of the problem to the desired result. Algorithms can be studied in a language- and machine-independent way [12].

Cyber attacks target to harm the communication and information systems. They would be most successful if make a breakthrough in management centers of critical infrastructure sectors. Therefore, the first step of the modelling and simulation process is building a computer network using a simulation software for network modelling like Riverbed Modeler Academic Edition 17.5, GNS3, Cisco Packet Tracer and etc. At this stage of the study the selection of compatible and conventional network devices and components is the most important action.

In this case the main steps in the modelling process of a typical management or control center are systematized in a cyclic type algorithm (Fig. 3). The optimal input parameters and components are described in Table 1. It is necessary to be noted that if the components are not compatible with each other, the simulation can not be correctly executed and the selected components must be changed with more suitable ones. When this is done the simulation should be restarted.

Table 1. Optimal input parameters and components

Input parameters	Network components
network size (X, Y)	Workstations
“delay”of the bus T_D	Servers
“thickness”of the bus	Switches

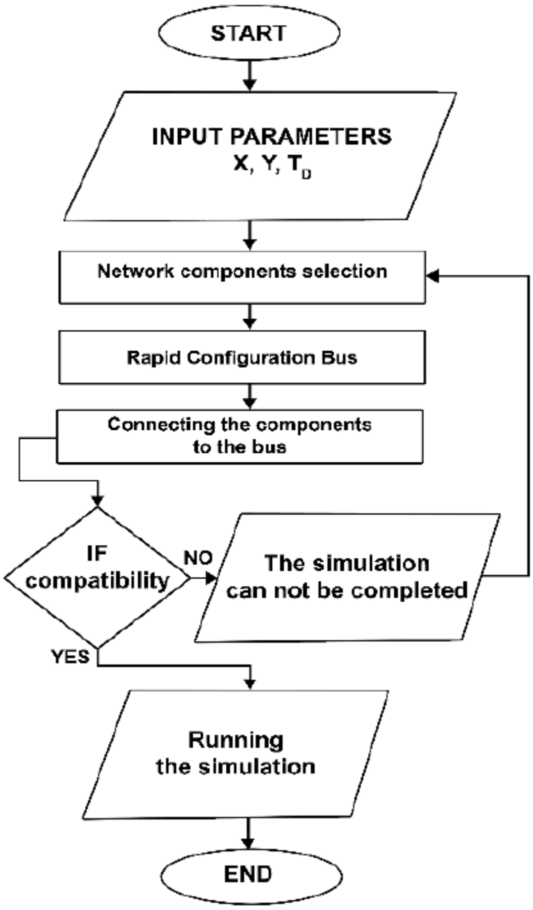


Fig. 3. Algorithm of modelling a management center.

In Fig. 4 is shown the second algorithm that presents the simulation of a DoS attack on the referent model of a management center - M_{Ref}. For reducing the negative impact of cyber attacks M_{Ref} should be optimized by a firewall insertion, reconfiguring the firewall or additional security settings like special security protocols and etc [13]. This is an experimental scenario aiming to prove that inserting a firewall ensures a better packet filtration and reduces the risk of flooding under the negative impact of a DoS attack. The optimal input parameters and generated output parameters are described in Table 2.

Table 2. Optimal input parameters and generated output parameters

Input parameters	Output parameters
“start time” T_0	sent traffic T_S
„ON State Time” - T_{ON}	received traffic T_R
“Interarrival Time” - T	maximum sent traffic $T_{S, max}$
simulation duration D	maximum received traffic $T_{R, max}$

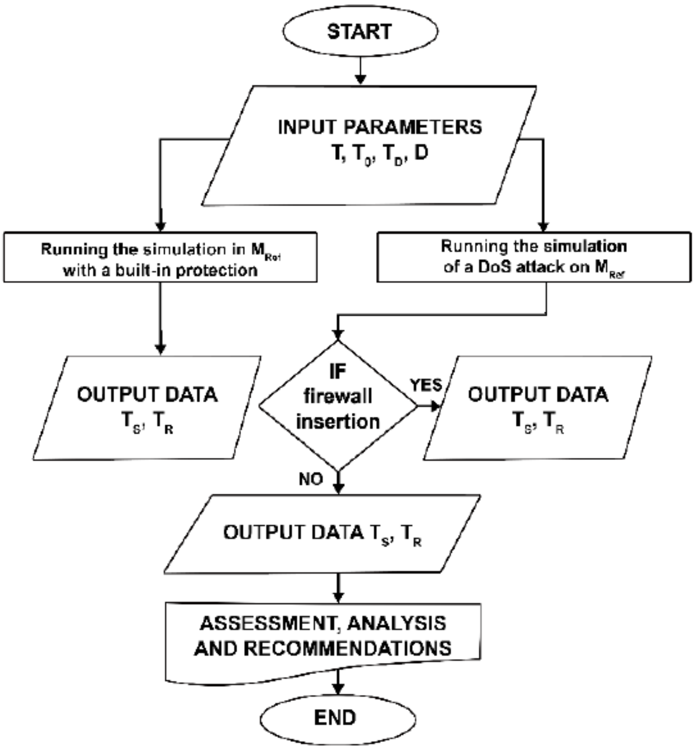

START
INPUT PARAMETERS
T, T0, TD, D
Running the simulation in MRef with a built-in protection
Running the simulation of a DoS attack on MRef
OUTPUT DATA TS, TR
IF firewall insertion
YES
OUTPUT DATA TS, TR
NO
OUTPUT DATA TS, TR
ASSESSMENT, ANALYSIS AND RECOMMENDATIONS
END

Fig. 4. Algorithm of simulating a DoS attack on a management center.

5. CONCLUSION

The effective protection of critical infrastructure requires a right approach for assessing the potential risk not only from physical but also from cyber threats, including the predicting possible negative consequences in case that a cyber attack has already been successfully realized. It is required means of protection to be considered in order the practical realization of cybersecurity policies to meet the expectations defined during the processes of planning and forecasting. Scientific and technological and the economic development of the countries are of decisive importance for developing effective methods and means of protection from threats of different strength and character for critical infrastructure.

The main advantages of the simulation modelling method make it one of the advanced means for ensuring correct data to address cybersecurity issues. The professional simulation systems have built-in libraries containing multiple models of actual network devices and components that can be configured by setting their specific parameters according to the the purposes of the study. One of the approaches for a verification of simulation models can be realized by a sequence of scenarios with different values of the reaction time.

In conclusion, its essence and designation explain why a comparison between the simulation results and confidential real data obtained using hardware prototypes can be avoided. Actually, if suitable algorithms are developed, simulation modelling is able to reduce the financial costs for tests in real environment [14], because of the need for a problem-solving methodology to support decision-making process, which is applicable in different areas.

REFERENCES:

1. Логистика – речник на използваните термини. *Военна академия „Г. С. Раковски“* [онлайн]. [прегледан 18 декември 2019]. Достъпен на: http://rndc.armf.bg; Logistika – rechnik na izpolzvanite termini. Voenna akademiya „G. S. Rakovski“ [onlayn]. [pregledan 18 dekemvri 2019]. Dostapen na: http://rndc.armf.bg

2. Закон за управление при кризи. Обн. ДВ, бр. 19 от 2005 г., изм. и доп., бр. 17, 30 и 102 от 2006 г. *АПИС* [онлайн]. [прегледан 18 декември 2019]. Достъпен на: https://web.apis.bg/ ; Zakon za upravlenie pri krizi. Obn. DV, br. 19 ot 2005 g., izm. i dop., br. 17, 30 i 102 ot 2006 g. APIS [onlayn]. [pregledan 18 dekemvri 2019]. Dostapen na: https://web.apis.bg/

3. НИКОЛОВ, Атанас и Иван ХРИСТОЗОВ. Корпоративна защита на информацията. Подход и решения. *Годишник Военна академия „Георги Стойков Раковски“*. София: Институт за перспективни изследвания за отбраната, 2005, с. 205-215. ISSN 1312-0816. ; NIKOLOV, Atanas i Ivan HRISTOZOV. Korporativna zashtita na informatsiyata. Podhod i resheniya. Godishnik Voenna akademiya „Georgi Stoykov Rakovski“. Sofiya: Institut za perspektivni izsledvaniya za otbranata, 2005, s. 205-215. ISSN 1312-0816.

4. НИКОЛОВ, Атанас и Иван ХРИСТОЗОВ. Проблеми и предизвикателства пред изграждането на национална система за киберсигурност. *Военен журнал*. 2015, год. 122(3), с. 7-13. ISSN 0861-7392. NIKOLOV, Atanas i Ivan HRISTOZOV. Problemi i predizvikatelstva pred izgrazhdaneto na natsionalna sistema za kibersigurnost. Voenen zhurnal. 2015, god. 122(3), s. 7-13. ISSN 0861-7392

5. Strengthening Cybersecurity in Europe. *European Commission* [online]. [viewed 18 December 2019]. Available from: https://ec.europa.eu/commission/index_en

6. Intelligent Agents. In: RUSSEL, Stuart and Peter NORVIG. *Artificial Intelligence A Modern Approach*. New Jersey: Prentice Hall, 1995, pp. 31-50. ISBN 0-133-601-242.

7. Probabilistic Reasoning Systems. In: RUSSEL, Stuart and Peter NORVIG. *Artificial Intelligence A Modern Approach*. New Jersey: Prentice Hall, 1995, pp. 436-467. ISBN 0-133-601-242.

8. Learning in Neural and Belief Networks. In: RUSSEL, Stuart and Peter NORVIG. *Artificial Intelligence A Modern Approach*. New Jersey: Prentice Hall, 1995, pp. 563-569. ISBN 0-133-601-242.

9. Neurons. *Simbrain 3.0 Documentation.* [online]. [viewed 19 December 2019]. Available from: https://www.simbrain.net/Documentation/docs/Pages/Network/neuron.html

10. НЕНОВА, Стефка Василева. *Методи и модели за изследване на комуникационните и информационните системи*. София: Найс АН, 2013. ISBN 978-954-8587-19-8. NENOVA, Stefka Vasileva. Metodi i modeli za izsledvane na komunikatsionnite i informatsionnite sistemi. Sofiya: Nays AN, 2013. ISBN 978-954-8587-19-8

11. BORSHCHEV, Andrei. *The Big Book of Simulation Modeling, Multimethod Modeling with AnyLigic 6*. AnyLogic North America, 2013. ISBN 978-0-9895731-7-7.

12. SKIENA, Steven S. *The algorithm design manual*. New York: Springer, 1998. ISBN 0-387-94860-0.

13. НИКОЛОВ, Атанас и Иван ХРИСТОЗОВ. Архитектура на център за реагиране на компютърни инциденти. В: *Годишник на Военна академия „Георги Стойков Раковски“.* София: Институт за перспективни изследвания за отбраната, 2006, с. 145-153. ISSN 1312-0816. NIKOLOV, Atanas i Ivan HRISTOZOV. Arhitektura na tsentar za reagirane na kompyutarni intsidenti. V: Godishnik na Voenna akademiya „Georgi Stoykov Rakovski“. Sofiya: Institut za perspektivni izsledvaniya za otbranata, 2006, s. 145-153. ISSN 1312-0816

14. CHEN, Ping, Lieven DESMET and Christophe HUYGENS. A Study on Advanced persistent threats. *Communications and Multimedia Security.15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings*. Springer, 2014, vol. 8735, pp. 63-72. Lecture Notes in Computer Science. ISSN 0302-9743.

Contacts:

Assistant, Eng.Yoana Atanasova Ivanova, New Bulgarian University, Department Telecommunication, Sofia, 21 Montevideo St., e-mail: yivanova@nbu.bg

Date of receipt of the manuscript: 26.07.2019.
Date of adoption for publication: 27.09.2019.