Годишник Телекомуникации 2022, том 9, с. 45-52

Yearbook Telecommunications 2022, vol. 9, p. 45-52

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

DOI: https://doi.org/10.33919/YTelecomm.22.9.4

A METHODOLOGY FOR EMPIRICAL RESEARCH AND ANALYSIS IN THE FIELD OF CYBERSECURITY

Yoana Ivanova

Abstract: This article is considered to be a continuation of a publication by the author devoted to an algorithm for steganographic embedding of encrypted files in raster images *(Yearbook Telecommunication, №9, 2022)*. The aim of this paper is proposing a methodology for empirical research and analysis on the field of cybersecurity which to contribute to various areas in cybersecurity. Its originality is expressed in the joint application of methods for research and analysis realized by various simulation environments for conducting experiments. This methodology has a specific structure as it is conditionally divided into two major parts depending on the type of the simulation process and software products used – a study of the direct impact of cyberattacks on communication networks by the method of the agent-based modelling and a study of potential steganography attacks using software for simulation of Artificial Neural Networks (ANNs) for the purposes of steganalysis.
Keywords: simulation modelling, steganography, steganalysis, artificial neural networks.

1. INTRODUCTION

Cybersecurity is broad field including various directions which can be explored in a virtual environment using the method of simulation modelling which can be realized by complex mathematical algorithms embedded in specialized software.

An example of such an algorithm is the backpropagation of error (BPE). It is used in ANNs for detection and classification of raster images because of its advantages. For example, one of the most advanced applications of this algorithm is in convolutional neural networks (CNNs). Neural networks are very useful in "stego-image" recognition. The mechanism of QR-steganography is interesting, because it is based on error correction after reading the QR (Quick Response)-code. When the specified image code numbers are replaced with numbers of the encrypted message *"the replaced codewords are considered as errors and are corrected by the error correction mechanism" [1]*.

Therefore, the methodology is based on a selection of powerful tools for simulation modelling of complex systems. Each software is applicable in a separate direction of cybersecurity for reducing costs and potential risks which are possible if the experiments are conducted in a physical environment. Besides the insertion of reliable input parameters in the simulation models and the verification and validation of the models are important to obtain accurate output results. There are different verification and validation techniques that can be used according to the methodological approach.

One of the key highlights of the article is pointed out as a solution for strengthen cybersecurity at the last stage of the methodology – OSINT (Open Source Intelligence) and forensics. Their main issues are explained by the use of a software suitable for education and training, as well as for professional analysis of cyber threats (MALTEGO).

The content of the article is divided into the following sections:

- ***Section II*** *summarizes good practices based on the experience gained during the work processes.*
- ***Section III*** *presents the conceptual framework and structure of the methodology proposed.*
- ***Section IV*** *is devoted to applications of a software product for OSINT and forensics in the field of cybersecurity.*

2. MAIN STAGES OF THE EMPIRICAL RESEARCH

A. Simulation modelling the impact of cyberattacks on communication networks

In Riverbed Modeler Academic Edition 17.5 various simulations can be performed such as simulations of DoS (Denial-of-Service) attacks on sectors of CI (Critical Infrastructure) and in particular on control centres of management systems such as TMS (Transport Management System).

There are two methods to simulate a DoS cyberattack in this environment: by the settings embedded in the element "cyber_effects" through the switch or by a jammer. In the first case a high level of protection can be ensured by a correct configured firewall between the attacker's workstation and the switch. If a DoS jamming is realized then the protection can be ensured by channel switching, because the pulsed jammer generates signals to "interfere with the correct signals coming from legitimate nodes and to occupy the transmission channel" [2].

B. Optimization of simulation models

One of the approaches is optimization by reconfiguring the firewall with security protocols (L2TP/IPSec). The conclusions are that although all the security measures in some of the ten scenarios a DoS can be implemented. Therefore, it is recommended machine learning algorithms to be implemented in applications for identifying and responding to cyberattacks before they to spread. The solution could be a model developed by big data analysis for security applications and identification of the mechanism of malicious activities [3, 4]. Therefore, the focus in this paper is on applications of AI (Artificial intelligence) and deep learning by ANN's as key components of the new generation of cybersecurity.

C. Applying advanced methods of steganalysis

- *steganalysis realization by using specialized software products*

Actually, the compression (KLT, Huffman coding) and then 6rs encryption (AES, DES, TripleDES) are the preliminary stages of this process. 7zip and CryptoForge are suitable software products for compression and encryption of a message, while the Karhunen-Loeve transform (KLT compression) can be performed in VSL (Virtual Steganographic Laboratory).

- *building ANN's for applications in steganalysis*

This stage of the methodology proposed is devoted to simulation modelling of Artificial Neural Networks (ANNs) with BPE for the purposes of cybersecurity.

BPE is a classical algorithm which is characterized by its optimal complexity and a comparatively fast realization especially in a specialized simulation environment such as SIMBRAIN. This is demonstrated in studies related to conducting a number of simulations for recognition of symbols, letters or segments of QR-codes even in case that the spatial orientations of the digital images are different. Therefore, another important advantage of the method can be defined as its ability to take into account all rotations and possible distortions, if necessary.

The author has used this simulation environment in research related to steganographic embedding by the main technique LSB (Least Significant Bit).

D. Creating agent-based visualizations in simulation environment

The visualizations in simulation software products are of three types: diagrams or/and tables (Riverbed Modeler) and 2D/3D agent-based visualization (Aimsun 8.0, NetLogo, Riverbed Modeler). In some simulation environments (NetLogo) it is possible to create or modify the program code and the visualization, respectively.

E. Establishing system measures of effective cyber protection

3. CONCEPTUAL FRAMEWORK AND STRUCTURE OF THE METHODOLOGY

The conceptual framework of the methodology for extensive research proposed by the author includes:

Годишник Телекомуникации 2022, том 9, с. 45-52

Yearbook Telecommunications 2022, vol. 9, p. 45-52

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

DOI: https://doi.org/10.33919/YTelecomm.22.9.4

- ***a methodological approach***

In this methodology the author applies a conceptual model validation based on the assumption that the knowledge underlying the concept are eligible and scientifically justified [5]. An example of such a claim is the linear bus topology of the typical control centres.

The computerized model verification is expressed in the correct programming and creating the model in simulation environment. For example, whether the model of a control centre consists of the right network devices and they are conventional and compatible, as well as if they are properly connected to the linear bus. The data validity is related to accuracy of the data required to build, evaluate, test and use the model.

The operational validation aims to prove that the simulation model is characterized by accuracy for its specific purposes within the intended applicability of the model. In this case is possible the simulation results to be compared to results obtained from experiments with hardware devices or simulation models, as well as the generated results from multiple simulation scenarios to be evaluated and analyzed. Actually, the changing of input parameters of a model recreates the variable behavior of a real system.

- ***a consideration of the applied methods***

The present study is characterized by the application of methods or their individual stages and variants, as follows:

- *empirical method* - formation (observation) and formulation (induction) of a working hypothesis; statements about the consequences of the hypothesis in the form of verifiable predictions (deduction); experimental proof of the hypothesis (test); evaluation of the results of the verification (evaluation).
- *experimental method* – it is expressed in conducting several series of experiments with selected software products for simulation modelling.

stochastic method - in the simulation modelling software used, the time and duration of the simulation are the main input parameters, which are entered before the start of the simulation and on which the generated results directly depend.

- *dynamic method* - the simulation products used provide an opportunity to take into account the interactions between the elements of the studied complex systems.

- ***preferable methods of analysis:***

- *comparative analysis* – it was used to draw important conclusions based on similarities and differences, advantages and disadvantages of two or more processes, data sets or simulation results.
- *logical analysis* - the author prefers the logical analysis to formulate summary estimates of the results, which are placed at the end of each experiment.

Fig. 1 presents a scheme of the methodology for empirical research and analysis in the field of cybersecurity.

4. OPEN SOURCE INTELLIGENCE (OSINT) AND FORENSICS

In this case “open source intelligence” means that software products from this type only examine public data that is available on the Internet. Such a product is MALTEGO which is designed for *“cybercrime investigations in law enforcement”*. According to its the applicable low “The jurisdiction of the Federal Republic of Germany applies to the legal information on this website as well as to all questions and disputes in relation to this website [6].”

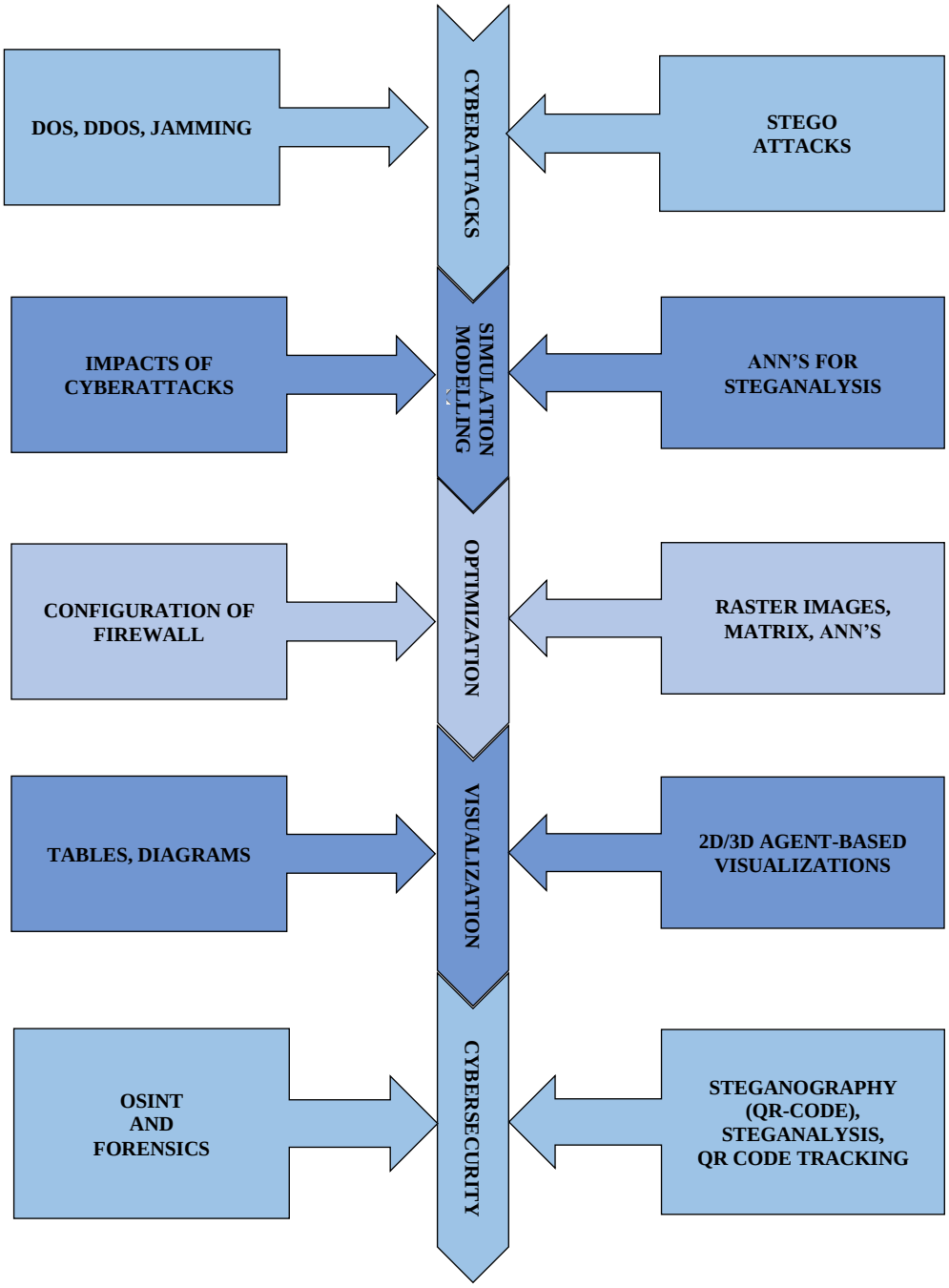

Fig. 1. A methodology for empirical research and analysis in the field of cybersecurity.

Fig. 2 represents the main characteristics of this useful application as follows:

- ***OSS (Open Source Software);***
- ***developed in Java;***
- ***graph-based*** *– „a graph is any ordered pair G = (V, E), where V is a set whose elements are called vertices, E is a set whose elements are called edges”,* such as [7]:

$$\boldsymbol{E} \subseteq \{\boldsymbol{X} \subseteq \boldsymbol{V} : |\boldsymbol{X}| = \boldsymbol{2}\} \qquad (1)$$

So, for each vertex $u \in$ V, the degree of u is $|d(u)|$ or the number of the neighbours N of u:

Годишник Телекомуникации 2022, том 9, с. 45-52

Yearbook Telecommunications 2022, vol. 9, p. 45-52

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

DOI: https://doi.org/10.33919/YTelecomm.22.9.4

$$d(u) = |N(u)| \qquad (2)$$

- ***Grey-Noise Intelligence*** – this is a solution that allows to filter the internet background noise and identify a cyber threat in order to reducing the risk [8].

Creating a new graph in MALTEGO includes some initial steps that are shown in the algorithm in Fig. 3.

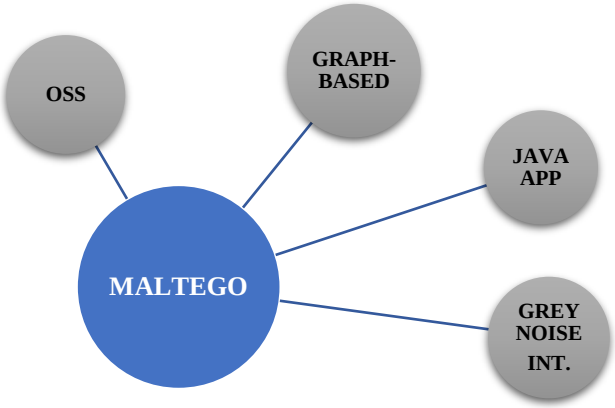

Fig. 2. The characteristics of MALTEGO.

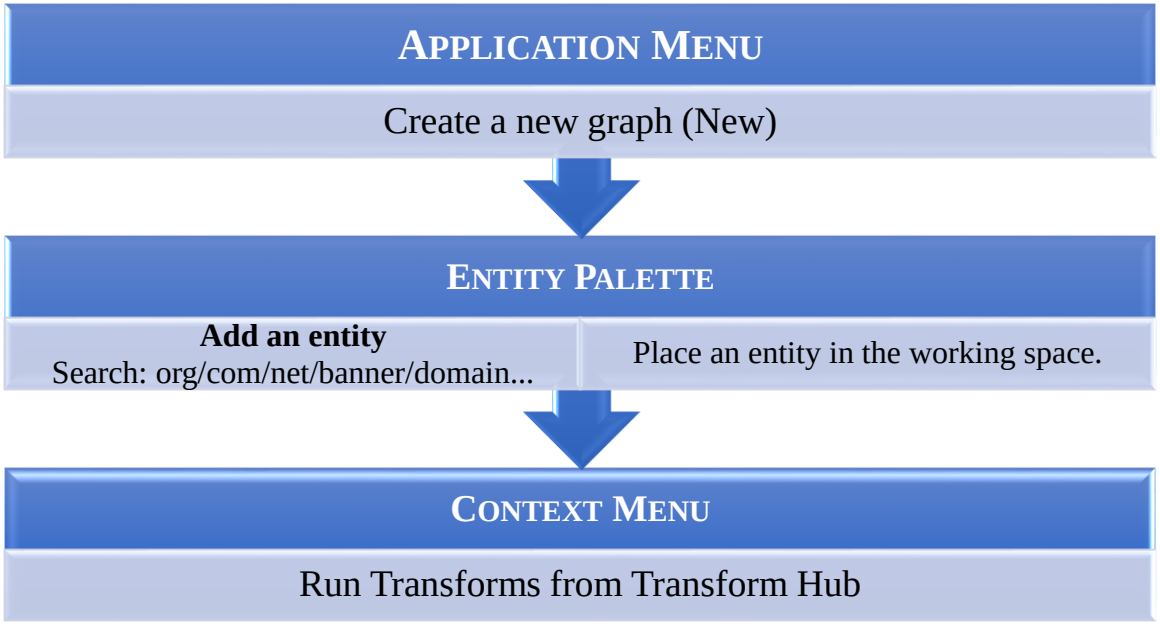

Fig. 3. An algorithm of initial steps to be performed in MALTEGO.

In Fig. 4 is shown a screenshot, representing some of the entities. Each entity can be transformed by right click and selecting *Change Type.*

Running transforms from the *Context Menu* means using *„functions which take an entity as input and create new entities as output. The output entities are then linked to the input entity“ [9].*

For example, the "threat intelligence" transforms aim to detect and analyze information for potential cyberthreats in order to strengthen the security of an organization. In the software they are represented as follows [10]:

- ***brand protection*** – *„finding websites masquerading as official websites from an organization"*.
- ***identifying the attacker;***
- ***mapping a malicious network;***
- ***threat intel.***

These objectives can be achieved by the functions *„IP Address [DNS]"* or *"To Domain"*.A conceptual example of a transformation process is shown in Fig. 5 for the entity *„Ipv4 Address"* (4x8-bits fields) that identifies a network interface on a computer and the transform formulated as *„To DNS name from passive DNS"*, searching for a DNS (Domain Name System) name, storing not only domain names, but also IP addresses.

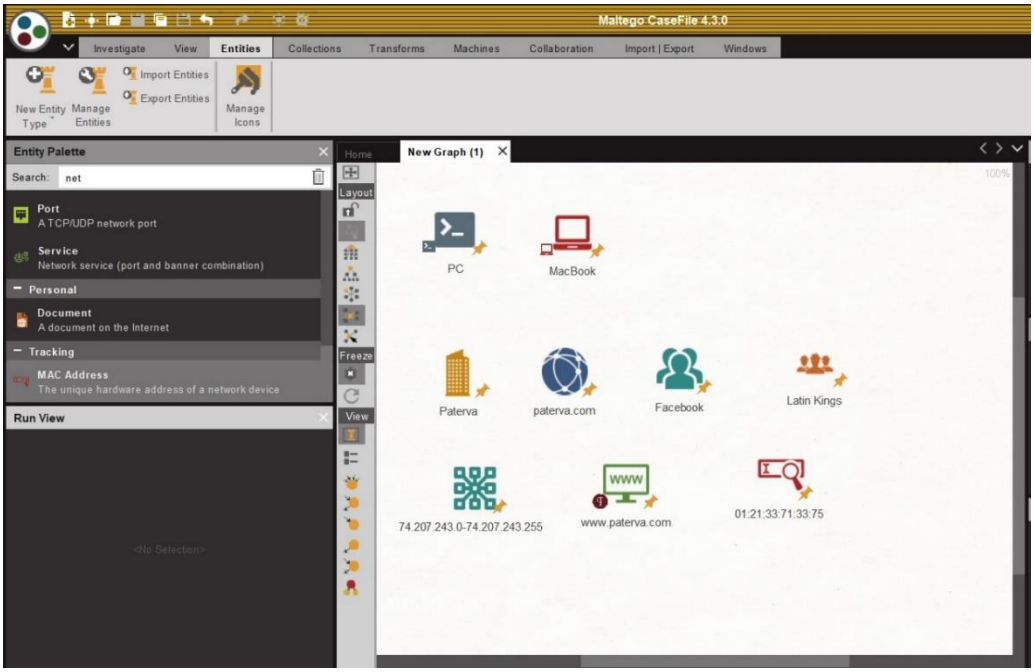

Fig. 4. Some of the entities in MALTEGO.

Fig. 5. A transformation of the entity „Ipv4 Address" into „To DNS name from passive DNS".

Годишник Телекомуникации 2022, том 9, с. 45-52

Yearbook Telecommunications 2022, vol. 9, p. 45-52

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

DOI: https://doi.org/10.33919/YTelecomm.22.9.4

The next example is related to the input entity *„E-mail Address“* and the relevant information related to it (Fig. 6).

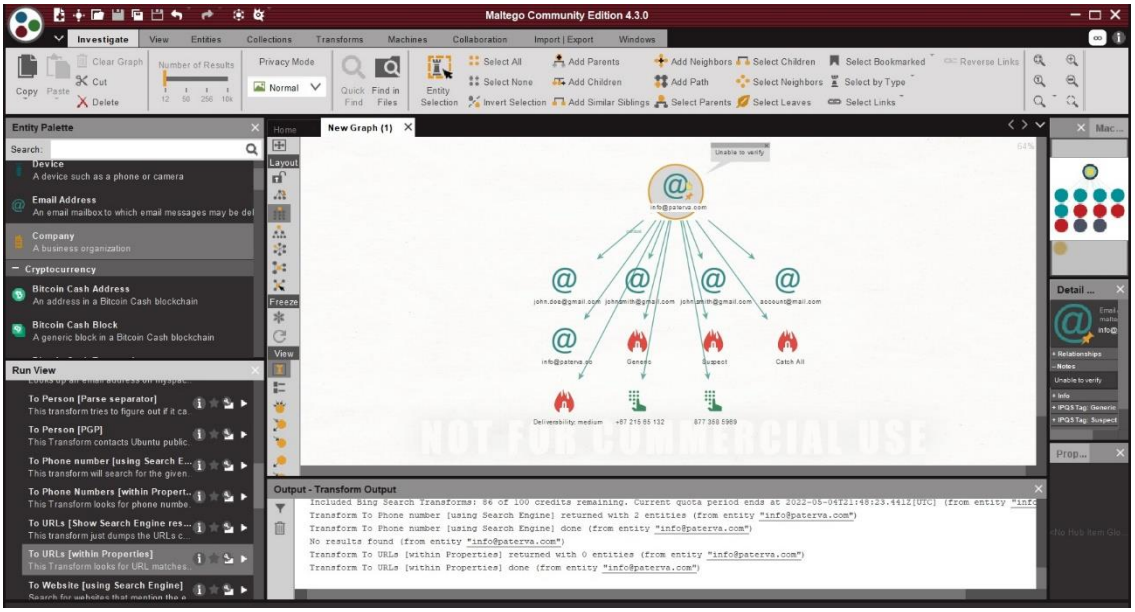

Fig. 6. The results of multiple transformations of the entity „E-mail Address”.

5. CONCLUSION

Actually, there is a great variety of methods and tools for performing detailed empirical research with a high level of scientificity. The ones presented in this paper are selected on the basis of advanced criteria for conducting a multilateral study such as a safe environment, an optimized process in terms of execution time and last but not least, reduced costs.

Besides, the methodology proposed has another advantage related to the possibility for insertion of additional modules if the comprehensive research acquires a new dimension and needs to be expanded in a different direction. In this sense CTI (Cyber Threat Intelligence) is a perspective area for study, because of the evolution of the threats. The growing need of new measures for cyber resilience is challengeing the developers of specialized software and researchers to join forces to minimize system vulnerabilities in order to achieve a higher level of cybersecurity.

REFERENCES:

[1] CUCURULL, Jordi, Sandra GUASCH, Alex ESCALA, Guillermo NAVARRO-ARRIBAS, and Victor ACIN. QR Steganography: A Threat to New Generation Electronic Voting Systems. *11th International Conference on Security and Cryptography (SECRYPT)* [online]. Vienna: IEEE, 2014, pp. 1-8 [viewed 20 January 2023]. eISBN 978-9-8985-6595-2. Available from: https://ieeexplore.ieee.org/document/7509529

[2] OBAID, Hadeel S. Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET. *Journal of Physics: Conference Series* [online]. 2020, vol. 1530(1), № 012009 [viewed 20 January 2023]. eISSN 1742-6596. IOPscience. Available from: DOI:10.1088/1742-6596/1530/1/012009

[3] КЪДРЕВ, Васил и Росен ПАСАРЕЛСКИ. Приложение на подходи на изкуствен интелект и машинно обучение в киберсигурността. *Годишник Телекомуникации 2021*[онлайн]. София: НБУ, 2021, (8), с. 53-64 [прегледан 20 Януари 2023]. eISSN 2534-854X. Достъпен на: https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii-broeve/godishnik-telekomunikacii-2021-g-tom-8 [KADREV, Vasil i Rosen PASARELSKI. Prilozhenie na podhodi na izkustven intelekt i mashinno obuchenie v kibersigurnostta. Godishnik Telekomunikatsii 2021[onlayn], Sofia: NBU, 2021, (8), s. 53-64 [pregledan 20 Yanuari 2023]. eISSN 2534-854X. Dostapen na: https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii-broeve/godishnik-telekomunikacii-2021-g-tom-8]

[4] СИМЕОНОВА, Цветелина и Васил КЪДРЕВ. Развитие на изкуствения интелект и неговото приложение в телекомуникационните мрежи и услуги. *Сборник доклади от Научна конференция с международно участие на НВУ „В. Левски", В. Търново, 27-28.05.2021*. Велико Търново: ИК на НВУ „Васил Левски, 2021, с. 2376-2386. ISSN 2367-7481. [SIMEONOVA, Tsvetelina i Vasil KADREV. Razvitie na izkustvenia intelekt i negovoto prilozhenie v telekomunikatsionnite mrezhi i uslugi. *Sbornik dokladi ot Nauchna konferentsia s mezhdunarodno uchastie na NVU „V. Levski", V. Tarnovo, 27-28.05.2021.* Veliko Tarnovo: IK na NVU „Vasil Levski, 2021, s. 2376- 2386. ISSN 2367-7481.]

[5] SARGENT, Robert, G. Verification and Validation of Simulation Models. *Proceedings of the 2010 Winter Simulation Conference* [online]. 2011, vol. 37(2), pp. 166-183 [viewed 20 January 2023]. eISBN 978-1-4244-9865-9. IEEE Xplore. Available from: https://ieeexplore.ieee.org/document/5679166

[6] Applicable Law. *Maltego* [online]. [viewed 20 January 2023]. Available from: https://www.maltego.com/legal-notice/

[7] МАРКОВ, Минко. *Лекции по теория на графите*, 2016. [MARKOV, Minko. *Lektsii po teoria na grafite*. 2016.]

[8] GreyNoise Intelligence Solution. *Maltego* [online]. 03 November 2021 [viewed 20 January 2023]. Available from: https://www.maltego.com/blog/greynoise-intelligence-solution-in-maltego/?fbclid=IwAR1pY36MqV7TI3BNNudoaxT9RJa6znZeNB4x5qCUpaKt66U7xmziO4_X73s

[9] Beginners' Guide Charting My First Maltego Graph. *Maltego* [online]. 03 June 2020 [viewed 20 January 2023]. Available from: https://www.maltego.com/blog/beginners-guide-to-maltego-charting-my-first-maltego-graph/

[10] Introduction to Maltego Standard Transforms. *Maltego* [online]. 18 August 2022 [viewed 20 January 2023]. Available from: https://docs.maltego.com/support/solutions/articles/15000041468-introduction-to-maltego-standard-transforms#overview-0-0

Contacts:
Chief Assistant, Dr. Yoana Atanasova Ivanova, New Bulgarian University, Department Telecommunications, Sofia, 21 Montevideo St., e-mail: yivanova@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 21.04.2022
Дата на приемане за публикуване (Date of adoption for pubication): 30.09.2022