МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2021
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2021
Proceedings of the Fiftieth Spring Conference
of the Union of Bulgarian Mathematicians
2021

A DECISION HIERARCHICAL MODEL OF CYBER SECURITY RISK ASSESSMENT*

Valentina Petrova

In this paper, the author introduce a multi-criteria decision making method to create a model of cyber security risk assessment to address cybersecurity issues according to the defined criteria. The method involves quantitative and qualitative approaches. The main goal is to present a model for cybersecurity and decision makers that ensure the confidentiality, integrity and availability of cybersecurity systems.

1. Introduction. The use of conventional security mechanisms is not always suitable, due to the requirements regarding confidentiality, integrity and availability. For that reason, the cyber risk assessment becomes inevitable part of system design and operation, which helps with the investment and operational decisions [5]. The main goals is to find an efficient way of cybersecurity risks assessment. Risks have dimensions and require specific measures. The risk assessment is recognized as a key component of managing security risks [8]. The risk assessment is the process of identifying, estimating, and prioritizing cybersecurity risks. Assessing risk requires very careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [13]. The process of conducting a security risk assessment involves two approaches: qualitative and quantitative. The quantitative cybersecurity risk analysis is used to include numerical values to all activities of the risk analysis process. The analysis is entered into the equation to determine the risk. This type of risk assessment is very complex, time consuming, expensive and is combined with qualitative approach. The qualitative approach goes through different scenarios for risk probabilities and threat rankings for evaluation of countermeasures. Qualitative assessment approach includes judgments and the experience of the assessor. There are no numerical values in qualitative risk analysis, but the risk is ranked on a hierarchical scale, e.g. *critical, high, medium* and *low.* The focus in this study is on the application of qualitative and quantitative risk assessment approaches [14].

2. An overview of application of multi-criteria decision making methods to create models of cyber security risk assessment. The most important models will be briefly analyzed where the application of multi-criteria decision making (MCDM) methods for the purpose of security risk assessment has been investigated. In paper [11] the authors propose a hybrid Information Security Risk-Control Assessment Model

*__2020 Mathematics Subject Classification:__ 62C05.
Key words: AHP, multi-criteria decision analysis, cybersecurity.

(ISRCAM) that includes three MCDM approaches (VIKOR, ANP and DEMATEL) to address conflicting criteria with interdependence and feedback. This model can help security managers to understand the control areas that need to be improved in order to get aligned with the acceptable level of risk (i.e. residual risk) per organization. Using the DEMATEL network relations map (NRM) technique, the model helps to analyze why certain security controls have more deficiencies (vulnerabilities). The risk management model is necessarily a continuous process based on the PDCA (Plan-Do-Check-Act) strategy. The proposed ISRCAM model examines the effectiveness of controls in the so-called "Check" phase. These two studies are very imporant because of use of the DEMATEL technique to map interdependencies between security elements. The Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted averaging (FLQ-MEOWA) operator is used to aggregate impact values assessed by experts, applied to diminish the influence of extreme evaluations such as personal views and drastic perspectives [6]. The TOPSIS method was integrated in the Identification of Existing Controls step during the risk analysis and identification process within the ISO/IEC 27005 risk management framework in [1,2]. Order performance by similarity to ideal solution (TOPSIS) method was utilized to determine the critical vulnerable controls on the basis of different evaluation criteria [1]. A hybrid procedure for evaluating the risk levels of information security under various security controls is proposed in [6]. This procedure applies the Decision Making Trial and Evaluation Laboratory (DEMATEL) approach to construct interrelations among security control areas. Ratings are obtained through the Analytic Network Process (ANP) method; as a result, the proposed procedure can detect the interdependences and feedback between security control families and function in real world situations. The Fuzzy Linguistic Quantifiers-guided Maximum Entropy Order-Weighted averaging (FLQ-MEOWA) operator is used to aggregate impact values assessed by experts, applied to diminish the influence of extreme evaluations such as personal views and drastic perspectives [6].

The authors of [12] identified four risk assessment factors. The AHP model for classification of information assets was presented. The paper did not specify to which systems the model would be applied and no necessary (inherent) interdependencies were defined between risk assessment factors.

3. An Analytical Hierarchy Process for cyber security risk assessment. An Analytical Hierarchy Process (AHP) represents the field of science called MCDA (Multi Criteria Decision Analysis), which is intended to assist the users in making decisions, defined as a *subjective measurement of various preferences* [9]. The main goal of the AHP method is dealing with complex decisions by giving them a rational structure, calculating the weight of the criteria and alternatives.

The AHP method is composed by the following stages:

Stage 1: The AHP was used to determine critical and vulnerable cyber security risks within systems based on a decision goal, criteria list and alternatives.

Goal: Identifying critical substations and estimating cyber security risks.

Criteria: The author proposed eight criteria named *attacks, vulnerabilities, penetration testing, threats, assets, security measures, unauthorized access*, and *security alerts.*

Alternatives: The alternatives are *confidentiality, integrity*, and *availability.*

The confidentiality, integrity and availability are considered the core underpinning of cyber security. The security control and vulnerability can be viewed in light of one or more of these key concepts.

Stage 2: The decision hierarchical model of cyber security risk assessment

The hierarchical structure is defined and described to support cyber security (Fig. 1):

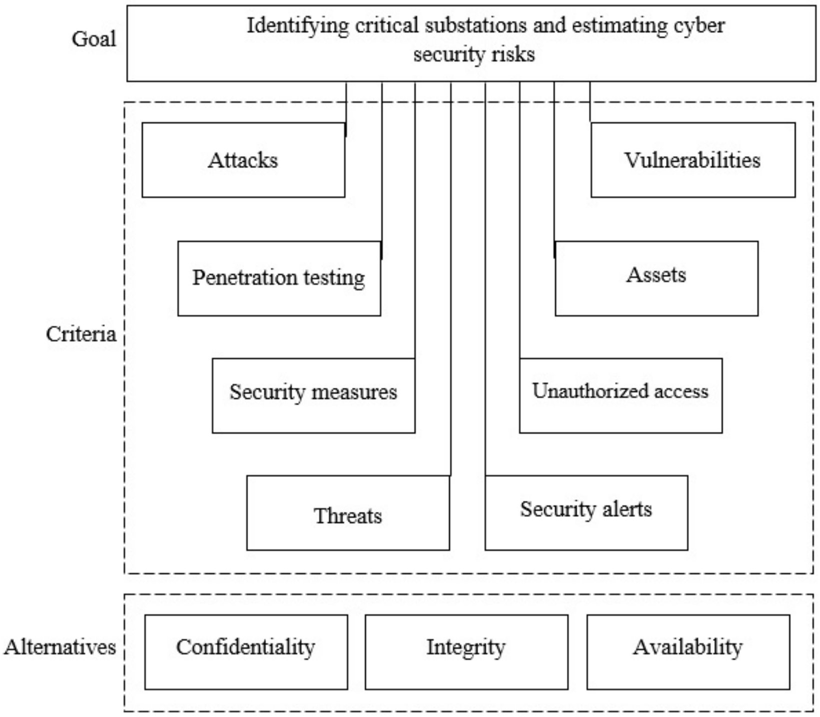

Fig. 1. The decision hierarchical model of cyber security risk assessment

The author presents the decision hierarchical model of cyber security risk assessment to evaluate and rank security incidents using the AHP whereby the eight decision criteria were the likelihood of an event and its consequences. The model reduces the number of risks and allows security analysts to focus on a critical incidents, which reduces the time and resources.

Stage 3: Mathematical implementation of the Analytical Hierarchy Process (AHP) method.

The AHP is a method of decision making using objective calculations based on evaluation of several criteria [10]. The AHP defines some stages of analysis [3]: the hierarchical structures formulation, prioritization, priority weight calculation of each criteria or alternative, and consistency checking. The hierarchical structure is defined by considering the scope, objectives, criteria, relevant actors, and alternatives [10]. Priority is a value that determines the level of importance of an alternative or criteria [3]. The AHP defines pairwise comparison to determine priorities using a matrix to compare variable of the same level in pairs. Comparisons were implemented using the Saaty preference scales

[ibid]. *Priority* weighting of each criteria or alternative is calculated using the Eigen value principle [4]. Consistency checking is performed to determine the likelihood of conflicting inputs. The inconsistency value should not be more than 10% [10].

4. Conclusion. The paper proposes a methodology to quantify a risk assessment of computer network security by using the AHP. The security risk analysis process has clearly indicated benefits of the proposed MSDM, in terms of precise risk assessment and higher return on cybersecurity investment. The method shows that AHP enables *fine* adjustment of the cybersecurity risk assessment process. The model reduces the overspending of resources in terms of cost and time and optimizes the assessment of cyber security controls themselves.

REFERENCES

[1] N. Al-Safwani, S. Hassan, N. Katuk. A multiple attribute decision making for improving information security control assessment. *International Journal of Computer Applications*, **89**, No 3(2014), 19–24.

[2] N. Al-Safwani, Y. Fazea, H. Ibrahim. ISCP: In-depth model for selecting critical security controls. Computers & Security, **77** (2018), 565–577.

[3] A. Ishizaka, P. Nemery. Multi-criteria decision analysis methods and software. Chichester, John Wiley and Sons, 2013.

[4] M. Khan, A. Parveen, M. Sadiq. A method for the selection of sdlc models using analytic hierarchy process. International Conference on Issues and Challenges in Intelligent Computing Techniques, IEEE, 2014, 534–540.

[5] D. J. Landoll. The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments. Auerbach Publications, Boca Raton, FL, US, 2006.

[6] C. C. Lo, W. J. Chen. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, **39**, No 1 (2012), 247–257.

[7] V. Petrova. Using the Analytic Hierarchy Process for LMS selection. CompSysTech '19: 20th International Conference on Computer Systems and Technologies, June 2019, Ruse, Bulgaria, 332–336, ISBN: 978-1-4503-7149-0.

[8] R. Roessing. An Introduction to the Business Model for Information Security. ISACA, 2010.

[9] T. Saaty. Theory and Applications of the Analytic Network Process, RWS Publications, 2005.

[10] T. Saaty, L. Vargas. Models, methods, concepts, and application of the analytic hierarchy process. New York, Springer, 2012.

[11] Y. P. Yang, H. M. Shieh, G. H. Tzeng. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, **232** (2013), 482–500.

[12] K. Zhang, L. Shao. Research on the quantitative methods of classified information system security risk assessment. International Conference on Logistics, Informatics and Service Science (LISS), Beijing, China, 571–575, 2014.

[13] `https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final`, accessed 17.02.2021.

[14] `http://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.100202`, accessed 17.02.2021.

Valentina Petrova
Information Technologies Department
Nikola Vaptsarov Naval Academy
73 Vasil Drumev Str.
9002 Varna, Bulgaria
e-mail: vmb75bg@gmail.com

ЙЕРАРХИЧЕН МОДЕЛ ЗА ВЗЕМАНЕ НА РЕШЕНИЯ, СВЪРЗАНИ С ОЦЕНКА НА РИСКА ПРИ КИБЕРСИГУРНОСТ

Валентина Петрова

В доклада авторът използва метод за многокритериално вземане на решения, за да създаде модел за оценка на риска при киберсигурност и да покаже неговото приложение при справяне с проблемите, съблюдавайки определени критерии. Методът включва количествени и качествени подходи. Основната цел е да се предложи модел, реализиращ конфиденциалност, интегритет и наличност, на разработчици, вземащи решения, свързани с осигуряване на киберсигурността.