УДК 621.396.99

Multi-Criteria Evaluation of Electronic Voting System Security Threats

Rasim Alguliyev[1], *Farhad Yusifov*[2]

Abstract. *E-voting system is one of the most important components of e-democracy. Implementation of the e-voting system has various purposes. Its main advantages are the selection of candidates with the appropriate competencies, increased activity and mobility of voters, participation of citizens in abroad and operative proclamation of election results and etc. Nowadays, security risks, threats play a vital role in the implementation and development of e-voting systems. There are many vulnerabilities related to different e-voting systems. In paper analysed the approaches to e-voting systems and the system security threats evaluation. An empirical evaluation of e-voting system security threats based on the multi-criteria evaluation approach (worst-case method and TOPSIS) is reviewed and the security threats are ranked based on appropriate criteria.*

Keywords: *E-democracy, E-voting, Internet Voting, Security Vulnerabilities, Threats, Multicriteria Evaluation, Worst-case approach, TOPSIS.*

Acknowledgment

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan - Grant № EİF-KETPL-2-2015-1(25)-56/05/1

DOI: 10.21681/2311-3456-2018-3-16-21

Introduction

E-voting is the most vital components of e-democracy covering actual research areas such as voting mechanisms, provision of security and legitimacy, technological solutions for e-voting and their efficient use. In a complex approach, e-voting is referred to an important part of e-elections [1-3].

Different approaches to voting types with the use of ICT are available in scientific sources, and there is a need for the unification of the terms used. Basically, the terms e-voting and Internet-voting are used to express online voting [2-6]. The term e-voting is broadly used, while Internet voting is only one of its forms.

E-voting has already been implemented by governments due to the rapid development of information technology and advanced cryptographic techniques. Nonetheless, taking into consideration the democratic principles, e-voting procedures and its security issues are still being argued. Transparency of the voting process in the political arena, calculation of votes in accordance with the democratic principles, protection of the rights of candidates and voters are of great importance.

The application of the e-voting system can influence the existing political processes in the country and is related to critical security systems [7]. From this point of view, identifying and evaluating the e-voting security threats is one of the topical issues for ensuring the transparency and citizen's involvement in democratic processes. In this study, the vulnerabilities in the e-voting system are explored and the evaluation of security threats to the e-voting system is considered.

E-Voting Systems: Views, Impacts and Approaches

In general, e-government creates new opportunities for development of democracy. It provides bilateral information relationship between citizens and civil society institution and public authorities with the application of ICT. In other words, e-government comprises the bilateral relations system of citizens, civil society and business-structures, and executive government structures through the use of the Internet. Implication of ICT in government performance, transparency and accessibility of government information, feedback principle between citizens and public authorities, government responsibility for the decisions made, and other issues in different countries are the main characteristics specifying e-government.

It is essential that the transition into the Information society, e-government strategy based on democratic values necessitates the gradual change of government model, the increase of share of civil and business structures, and the minimization of government share

According to the concept of e-government, the whole system of public authorities functions as an integral service organization for the provision of services to citizens. The performance of e-government must be clear, transparent and accessible in terms of information for citizens. The specific attention is drawn to the establishment of feedback mechanism, efficiency of services provision and execution period by using the centralized systems. These all enable to increase either the quality of provision of services provided by the government to citizens, or the performance efficiency of government.

In practice, the diversity in opinions regarding the use of e-voting systems is still observed. Although some

1. Rasim Alguliyev, Dr.Sc., Director of the Institute of Information Technology of Azerbaijan National Academy of Sciences (ANAS) and academician-secretary of ANAS, Baku, Azerbaijan. E-mail: r.alguliev@gmail.com
2. Farhad Yusifov, Ph.D., Head of department of Institute of Information Technology of ANAS, Baku, Azerbaijan. E-mail: farhadyusifov@gmail.com

countries consider the implementation of e-voting as more efficient by presenting various arguments, other countries propose the reverse.

As a new concept, the implementation of e-voting is based on reducing errors during election processes and focus on maintaining the integrity of election process in general. In literature, e-voting is defined as a use of computers and devices offered by computers in election process, and this term is adopted to characterize elections carried out via the Internet more precisely [1].

E-government system allows enhancing the accessibility of all government services and operations in accordance with the interests of citizens, organizations, employees and other interested parties, and maintaining accessibility for everyone and fostering the efficiency by transforming the system of regular provision of public services. On the other hand, e-democracy is defined as "the use of the Internet as a tool for the democratic election of political leaders and government policies" [1]. The main characteristics of e-democracy are considered as the expansion of political information, e-voting and the participation in e-decision making. While defining e-democracy in the categories of e-government, it is seen as more appropriate for relations between citizens and government in accordance with G2C model [1,8].

Development of e-voting, public forums, open government, public opinion analysis is the basis of e-democracy formation [8]. E-democracy, particularly e-voting, has led to broad discussions in practice and literature [2-5,9]. As the major discussion topics, the security issues and the impact of e-voting on socio-political processes are highlighted [6]. Therefore, security issues play a crucial role in the application of e-voting systems. Voting is viewed as a system that is characterized by the participation of citizens in democratic processes and forming the general opinion. However, it can be noted that e-voting is more complex and sensitive system. Security of the election process must be considered at the national security level. Because, legitimacy of democracy depends on the transparency, openness and trustworthiness of elections. From this point of view, e-voting system has commitments in society, and its failure can lead to serious problems related to the confidence of citizens in political processes [6,9].

To facilitate e-voting and to ensure its more efficient and inexpensive realization, it should be implemented in the following two forms with the use of electronic tools: supervised e-voting - requires a representative of government or electoral authority and/or remote e-voting - does not require an observation by the representative and can be implemented via the Internet voting or mobile devices [3,6,7,9]. In the context of remote e-voting via the Internet, e-voting solutions in the literature are grouped into three major categories: kiosk voting, Internet voting in the voting center, and remote Internet-voting [6,9]. Although different approaches to e-voting are available today, it is believed that mobile voting solutions are estimated to be developed in the near future taking into account the factors urging e-voting.

Implementation of the e-voting system may reduce the errors occurred in the election process, ensuring the comprehensiveness, transparency, and convenience of the election process. Despite the advantages of using the e-voting system, this process is accompanied by numerous social, legal and technical problems. Moreover, the problems may also include the provision of equal access to voter centers, confidentiality, prevention of intervention, threat evaluation, verification, modification and approval of other procedures, universal confirmation, voting right, preservation of the principle of "one voter and one vote", and error resistance. From this point of view, the inevitability of transforming legal restrictions into technical and security solutions should be emphasized. The factors imposing e-voting are:

E-democracy development: Developing efficient e-voting mechanisms is crucial for forming and developing e-democracy. Government agencies, political parties, and politicians focus on e-voting as a powerful tool for ensuring democratic principles. E-voting is of great importance in terms of eliminating digital divide in the developing countries that initiate the democracy, establishing close links between provinces and centers, preserving democratic values and holding fair elections.

Security: One of the most argued issues in the application of the voting system is security [10-14]. Obviously, in the traditional election system, it is impossible to identify voters by their votes. Because, the election process is carried out through secret ballot, and each voter drops the attached envelope into the ballot box. Each voter follows the principle of confidentiality. However, this does not mean the transparency of the election process. For example, a voter has no guarantees that his/her voice will not be changed later. Despite the e-voting efforts to ensure security, e-voting is considered as a real threat to the confidentiality of personal data.

Transparency failure: Undoubtedly, ensuring security requirements with information technology, and even using cryptographic techniques and tools promotes transparency in the election process. However, it is uncertain whether the voters will have difficulties to accept and follow safety requirements or not [2,4-6,11,12].

Election fraud: It should be noted that security of traditional elections is based on the human trust and independence of election committees. Previous experiences reveal that in developing countries with emerging democratic rules, the trust in these mechanisms is low. Therefore, transition into technical security, i.e., cryptographic coding may be more effective rather than the organizational security. It should be noted that the joint use of organizational and technical security tools is gradual. In other words, if the organizational authorities are corrupted, even the most reliable technology can be abandoned. Additionally, joint use of organizational and technical security measures will gradually have the same character [3,11,15,16].

Voter participation: The impact of E-voting on the voter attendance is expected to be characterized not only by the voting form, but also by the relevant cultural, political and geographical conditions. For example, low density of the Australian population, migration of majority of Estonian population to other European countries due to unemployment, the resettlement of voters in the countries of political conflict or war, etc.

Eliminating invalid votes: Invalid votes may be intentional and unintentional stemmed from technical issues.

Fraud of votes is regarded as a step contradicting the democratic principles. The increase in the number of invalid votes puts the election results under suspicion.

Invalid votes in the e-voting process can be detected during inspection. Adjustments to the software through feedback can minimize the number of invalid votes. From this point of view, this kind of obstacles, which restrict the democratic "equality principle," should be officially investigated whether they are legitimate or not [1,2,16,17].

Cost saving: The costs can be minimized with the physical presence in voting and the minimal number of staff recruitment or reductions in travel costs. On the other hand, building voting system requires providing the voters with the necessary technical equipment. In addition, in the near future, the polling stations will lose their power in political elections. Despite all this, e-voting is still argued in terms of saving money spent on election.

In general, can be noted that the legal framework for elections is extensively argued, and consequently, it is believed that the legal solution of the problem is related to the transition from law to technology.

E-Voting System Vulnerabilities

Modern democratic countries hold elections through e-voting system. The use of ICT makes the electoral process more effective in terms of voting and increasing the number of voters. This is explained by the fact that e-voting facilitates and supports the voting process. The main contribution of e-voting and, in particular, Internet-based voting systems, is the voters' mobility support, which in turn enables voters to attend elections from anywhere via the Internet access. The key gaps associated with e-voting are related to the voter authentication and, principally, threats to the Internet voting software, such as viruses, malware, and Trojan horse [7]. Internet voting issues may include completeness of voter information, reliable transfer and storage of votes, prevention of vote duplication and so forth [7,9,12-14].

There are many vulnerabilities related to different e-voting systems [2,3,5,7,17]. Most available e-voting systems are not satisfactory for holding reliable elections since current practice shows that there is no evidence to prove their truthfulness. The main reason for the restricted implementation of e-voting is the lack of confidence. However, in the near future, the development of effective mechanisms promises more reliable e-voting. E-voting system is grouped into 3 main categories: hardware, software and human factor. The safety elements of hardware include electromechanical and electrical parts [2]. Security features of the software include operating systems, compilers, databases, software rules, and so on. Ease of use, transparency, confidence, and adoption are the security elements for human ware or voter. In literature and practice, each category is equally important in terms of safety [2,14].

Regulation of functional and constitutional obligations by the state leads to dealing with numerous problems of the e-voting system. From this point of view, the e-voting system must totally meet the electoral principles. This approach becomes a security requirement for the technological solution and must be implemented in the voting environment. Technical and security features of effective e-voting system include accuracy, verification, democratization, agility, mobility, reliability, consistency, public acceptance, etc. Other desired requirements include comfort, transparency, measurable and economic feasibility. Although there are various approaches to e-voting security in the scientific literature, most of the above requirements are unambiguously accepted by researchers [1,16-19]. However, some of requirements are controversial. For example, the controversy emerging the conflict between authentication and confidentiality is the requirement to verify whether the voter has the right to vote or not, including the requirement to provide the confidentiality of the voter's vote.

E-Voting Security Threats

Research in the field of e-voting is considered to be one of the important aspects of the development of e-democracy mechanisms. Establishing a comfortable and secure e-voting system can become a powerful tool for gathering people's ideas and opinions in cyberspace. E-voting system can be attacked in different ways. Threats can cause the system failure by affecting its different security areas. Potential e-voting system threats may include the followings [7,10,11,13,17]:

Technical vulnerabilities. Software developers or system administrators create an inaccessible administrator account for operators. Administrator account is used for troubleshooting, prevention of system errors, or for personal purposes. These accounts can be hijacked and used for malicious purposes. These vulnerabilities are referred to technical threats.

Denial of Service - DoS attack. DoS attacks cause destructive results and, in most cases, affect the system stability making it inaccessible. Hackers may endanger e-voting system access using various methods, including the Ping of Death and Packet Flooding. These types of attacks do not affect all systems in the same way. Thus, some systems may stop functioning, while others may not be affected at all.

Viruses. A computer virus is a computer program with self-recover function and causes undesirable effects on computers where it is activated. Viruses can destroy the e-voting system. A virus attack can jeopardize the system access in the course of an election and force the government and institutions to hold the re-election. Attacks on emails are most common attacks and referred to technical threats.

Worms. These viruses are spread without modifying available programs and files. It spreads to become active in other systems by creating own copies on infected computers. If a virus is intentionally developed, it may invalidate elections by changing files and voting results.

Trojans. The Trojan horse virus is a malicious program code downloaded once the computer is connected to the Internet. At the first glance, this virus can seem undisruptive; however, it may delete an important file on the computer, create a malicious virus, and even seize user passwords. This virus is a serious threat to the data integrity and confidentiality in the e-voting system.

Phishing. Some phishing swindlers develop forged Web pages similar to legitimate ones and illegally get voter information, and misrepresent election results using their rights. This threat may be related to both technical and social categories depending on the type of attack.

Physical attacks. Numerous physical attacks to e-voting system can be realized to disrupt the electoral process. Malefactor's access to the Internet and interference to the power supply can ultimately lead to the loss of votes. Hard drive or smart-card removal or substitution with fraudulent data, and capturing voter's personal data is a serious threat to e-voting process.

Threats to the integrity of computing subsystem and system. Computing subsystem attacks may falsify and alter it through the client software or the server in accordance with the malefactor's request. This threat can be classified into both technical and social threats.

Threats to User computer. In scientific literature, compared to other operating systems, the Windows system is estimated to have more vulnerabilities. When updating any popular software in the Windows environment, the viruses such as Trojan horse and backdoor can be invisibly uploaded to the computer while the user computer is run for various purposes. Widespread use of this operating system and the availability of numerous gaps and being easily defined by hackers may cause a serious threat to e-voting.

E-Voting Security Threats Evaluation

In general, it is known that selecting the best alternative among many alternatives is a multi-criteria decision making (MCDM) problem [20-27]. MCDM is one of the most widely used decision methodologies in different fields. A typical MCDM problem involves a number of alternatives to be evaluated and a number of criteria to evaluate the alternatives [21-23,25]. MCDM methods deal with problems of compromise evaluation of the best solutions from the set of available alternatives according to objectives. In this study, comparison of the results was proposed for e-voting security threats evaluation using three criteria on the basis of models of worst-case approach [21] and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [23].

Numerical Study: Worst-Case Approach + TOPSIS.

Assume that local elections are decided to be held via e-voting system. The ranking of e-voting system threats using the multi-criteria evaluation method is reviewed. The following four threats are predicted to e-voting system: $A=\{A_1,A_2,A_3,A_4\}$.

Here, denotes the DoS attacks (A_1), virus attacks (A_2), phishing threats (A_3), and physical attacks (A_4).

The criteria used to evaluate the threats are as follows: $C=\{C_1,C_2,C_3\}$, denotes the system interruption (C_1), violation of data integrity and confidentiality (C_2), falsification of election results (C_3).

The idea of the worst-case method [21] is borrowed from structural system analysis, where the reliability of a system is distributed among its elements (or alternatives) according to their ranks. This approach compares alternatives only with the one that is the least important among them.

Step 1. If the Saaty (2008) approach is used, then the ranking $\frac{R_i}{R_l}$ of alternatives on each criterion $c_j \in C$ can be shown as follows. Here, A_l - is the worst l -th alternative among the alternatives A_i ($i=1,4$).

$$\frac{R_i}{R_l}=\begin{cases} 1, \text{ if equal importance to } A_i \ A_l, \\ 3, \text{ if relatively weak importance than } A_i \ A_l, \\ 5, \text{ if strong importance than } A_i \ A_l, \\ 7, \text{ if very strong importance than } A_i \ A_l, \\ 2,4,6 - \text{intermediate values.} \end{cases}$$

Evaluation of each threat by criteria is shown in Table 1.

Table 1. Evaluation of threats by criteria

	C_1	C_2	C_3
A_1	7	5	2
A_2	5	1	3
A_3	3	6	1
A_4	1	4	7

Step 2. Assume that alternative A_l is the worst alternative with weight w_l and rank R_l. Using the worst-case method, the weight of the worst alternative for each criterion is calculated using the following formula [21,25]:

$$w_l=\frac{1}{\sum_{i=1}^{4}\frac{R_i}{R_l}}$$

According to the worst-case method, the condition $w_1+w_2+...+w_l=1$ is met and the weights of remaining alternatives are calculated [21]. Table 2 shown the weight of alternatives calculated through the worst-case method. The calculated weight of alternatives by criteria allows to expressing the criteria as fuzzy universal sets [21].

Table 2. Weights of alternatives calculated through the worst-case method

	C_1	C_2	C_3
A_1	0,438	0,333	0,154
A_2	0,313	0,067	0,231
A_3	0,188	0,400	0,077
A_4	0,063	0,200	0,538

Step 3. According to the Belman-Zadeh principle, the best alternative (A_{opt}) can be found within the intersection of the fuzzy sets of these criteria [21].

Then, intersection $A_{opt} \in D=C_1 \cap C_2 \cap C_3$ builds a fuzzy set. According to the fuzzy sets theory, the maximum weighted alternative $A_{opt} \in D$ is chosen as the best alternative (A_{opt}) by replacing the intersection with $\cap \to \min$. As can be seen in Table 3, alternatives are ranked in the following sequence: A_1, A_3, A_2 and A_4.

Table 3. E-voting threats ranking

	D worst-case	Rank
A_1	0,154	1
A_2	0,067	3
A_3	0,077	2
A_4	0,063	4

Step 4. According to Zadeh (2016) approach, alternatives can be ranked by the importance of criteria taking the weight coefficients $\alpha_1 = 0.6$ (very important), $\alpha_2 = 0.3$ (important) and $\alpha_3 = 0.1$ (less important). The weights of alternatives are shown below.

$$D^{\alpha} = \left\{ \frac{0,015}{A_1}, \frac{0.0}{A_2}, \frac{0.008}{A_3}, \frac{0.038}{A_4} \right\}$$

As it is seen, threats are ranked by the importance of criteria in the following sequence A_4, A_2, A_1 and A_3.

The TOPSIS method is based on the intuitive principle that the best alternatives should have the minimum distance from the positive-ideal alternative and the maximum distance from the negative ideal alternative [22,23]. This method has been widely used in various MCDM models for solving practical decision problems [22,23,25]. Using evaluation values of each threat by criteria which is shown in Table 1 can be implemented TOPSIS method for ranking e-voting threats. The TOPSIS method consists of the following steps [23,25]: 1) Construct a decision matrix for the ranking; 2) Normalize the decision matrix; 3) Determine the positive-ideal solution and negative-ideal solution; 4) Calculate the distance of each alternative from the positive-ideal solution and negative-ideal solution; 5) Calculate the closeness index of each alternative; 6) Rank the alternatives.

Alternatives A_i are ranked in descending order based on C_i value and select the alternatives with highest C_i value. The closeness index C_i shows the Euclid distance to the positive ideal solution, as well as the negative ideal solution. The closeness index C_i for each alternatives is calculated as following [23,25]:

$$C_i = \frac{D_i^-}{D_i^- + D_i^+}, \quad i = 1,2,\ldots,n$$

Based on the Euclid distance of each alternative from the positive ideal solution $D_i^+ \geq 0$ and negative ideal solution $D_i^- \geq 0$, it is clear that the value of C_i is between 0 and 1. Higher the index value of C_i the better performance of alternatives.

If implement this steps according to evaluation data of each threat by criteria is shown in Table 1, the threats ranking with using TOPSIS method are shown below (Table 4).

Table 4. E-voting threats ranking using TOPSIS method

	DTOPSIS	Rank
A_1	0,561	1
A_2	0,449	3
A_3	0,437	4
A_4	0,518	2

As it is seen, threats are ranked by the importance of criteria in the following sequence A_1, A_4 A_2 and A_3.

Conclusion

E-voting is distinguished from any other electronic transaction for its significance. Violation of the right to secret ballot in e-voting can lead to political conflicts and social disorder. From this point of view, e-voting is a real threat to the confidentiality of personal data. The problem of phishing, viruses, and spy programs still remain a serious threat to voters and e-voting system. In the paper examined the approaches to e-voting system and factors that made the system and its security threats more relevant.

Based on the multi-criteria evaluation method, the weights of all alternatives (threats) were calculated using the worst-case method for solving the issue of empirical evaluation of e-voting system security threats and the threats were ranked based on Belman-Zadeh's principle. TOPSIS method was used here for comparing the results of threats ranking. If compare among these methods, TOPSIS method seemed to be more appropriate for solving the security threats evaluation problem because it has the capability to deal with each kind of judgment sub-criteria and criteria. In particular, proposed approaches can be used as a hybrid (worst-case and TOPSIS) methods. Further studies will focus on the development of hybrid MCDM method to solve the alternatives ranking problem.

Based on the analysis of extant practices in the field of e-voting, it can be concluded that e-voting system security threats at the local level should be assessed and empirical research should be preferred. This issue is particularly urgent and important for developing countries. Given the security features of e-voting system, e-voting mechanisms to be developed will allow solving numerous problems.

Reviewer: *Valentin Tsirlov, Ph.D., Associate Professor, Information Security Department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: v.tsirlov@bmstu.ru*

References

1. Abu-Shanab, E., Knight, M. and Refai, H. (2010). E-voting systems: a tool for e-democracy management research and practice, Management research and practice, 2(3), 264-274.
2. Mursi M., Assassa G. and et al. (2013). On the Development of Electronic Voting: A Survey, International Journal of Computer Applications, 61(16), 1-13.
3. Wang, K. H., Mondal, S. K., Chan, K. and Xie, X. (2017), A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability, Data Science and Pattern Recognition Ubiquitous International, 1(1), 31-47
4. Schryen, G. (2004). Security Aspects of Internet Voting, Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04), 2004, https://www.ssrn.com

5. Musial-Karg, M. (2014). The use of e-voting as a new tool of e-participation in modern democracies, http://www.pressto.amu.edu.pl
6. Warkentin, M. Sharma, Sh. Gefen, D. (2018). Social identity and trust in internet-based voting adoption, Government Information Quarterly, https://doi.org/10.1016/j.giq.2018.03.007
7. Li, X.Sh., Lee, H.R., Lee, M. and Choi, J.-Y. (2015). A Study of Vulnerabilities in E-Voting System, Advanced Science and Technology Letters, 95, 136-139.
8. Van der Meer, T. G.L.A., Gelders, D. and Rotthier, S. (2014). E-democracy: exploring the current stage of e-government, Journal of Information Policy, Penn State University Press, 4, 489-506.
9. Stoica, M., Ghilic-Micu, B. (2016). E-Voting Solutions for Digital Democracy in Knowledge Society, Informatica Economică, 20 (3), 55-65.
10. Lauer, T.W. (2004). The Risk of e-Voting, The electronic journal of e-government, 2 (3), 147-218.
11. Ssekibuule, R. (2007). Security Analysis of Remote E-Voting, Advances in Systems Modelling and ICT Applications, http://www.cit.mak.ac.ug
12. Al-Ameen, A. and Talab, S. (2013). The Technical Feasibility and Security of E-Voting, The International Arab Journal of Information Technology, 10(4), 397-404.
13. Javaid, M.A. (2014). Electronic Voting System Security, https://www.papers.ssrn.com
14. Schneider, A. Meter, C. Hagemeister, P. (2017). Survey on Remote Electronic Voting, https://arxiv.org/abs/1702.02798
15. Kang, B. (2008). Cryptanalysis on an e-voting scheme over computer network, International conference on computer science and software engineering, 826-829.
16. Cetinkaya, O. and Cetinkaya, D. (2007). Verification and Validation Issues in Electronic Voting, The electronic journal of e-government, 5(2), 117-126, http://www.ejeg.com
17. Dhillon, K. (2015). Challenges for LargeScale Internet Voting Implementations, http://www.cs.princeton.edu
18. Qadah, G.Z. (2007). Electronic voting systems: Requirements, design, and implementation, Computer standards and interfaces, 29 (3), 376-386.
19. Okediran, O.O., Omidiora E.O. (2011). A Framework for A Multifaceted Electronic Voting System, International Journal of Applied Science and Technology, 2011, vol. 1 (4), pp. 135-142.
20. Saaty, T.L. (2008). Decision making with the analytic hierarchy process, International Journal of Services Sciences, 1(1), 83–98.
21. Rotshtein, A.P. (2009). Fuzzy multicriteria choice among alternatives: Worst-case approach, Journal of Computer and Systems Sciences International, 48 (3), 379-383.
22. Kelemenis, A., Askounis, D. (2010). A new TOPSIS-based multi-criteria approach to personnel selection, Expert Systems with Applications, 37, 4999–5008.
23. Chang, Y.-H., Yeh, C.-H., & Chang, Y.-W. (2013). A new method selection approach for fuzzy group multicriteria decision making. Applied Soft Computing, 13(4), 2179–2187. doi:10.1016/j.asoc.2012.12.009
24. Khorami, M., Ehsani, R. (2015). Application of Multi Criteria Decision Making approaches for personnel selection problem: A survey, International journal of engineering research and applications, 5(5), 14-29
25. Alguliyev, R.M., Aliguliyev, R.M., Mahmudova, R.M. (2016). A Fuzzy TOPSIS+Worst-Case Model for Personnel Evaluation Using Information Culture Criteria, International Journal of Operations Research and Information Systems, 7 (4), 38-66.
26. Tuan, N.A. (2017). Personnel Evaluation and Selection using a Generalized Fuzzy Multi-Criteria Decision Making. International Journal of Soft Computing, 12 (4), 263-269.
27. Afshari, A.R., Nikolić, M., Akbari, Z. (2017). Personnel selection using group fuzzy AHP and SAW methods, Journal of engineering management and competitiveness, 7(1), 3-10
28. Zadeh, L.A. (2016). A Very Simple Formula for Aggregation and Multicriteria Optimization, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 24 (6), 961–962.