**Yadigar N. Imamverdiyev**
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az
DOI: 10.25045/jpit.v09.i2.04

# A CONSENSUS RANKING METHOD FOR INFORMATION SECURITY THREATS OF AN E-GOVERNMENT

*Threats to information security of the e-government are aimed at national interests in the information sphere. There are many threats to national interests in the information sphere, and in order to effectively counter these threats in the face of limited resources allocated to cyber defense, multi-criteria ranking of these threats is necessary. In the proposed model, threats are ranked on the basis of expert assessments that characterize the levels of threats to national interests. An optimization model for consensus threat ranking is proposed.*

***Keywords:*** *e-government, information security, information security threats, threat assessment, threat ranking, consensus ranking.*

## Introduction

Ensuring information security is one of the most important issues of domestic and foreign policy of any state [1]. Information security of the state can be defined as the condition of national interests in the field of information. The field of information embraces a system that regulates the subjects forming information, government information infrastructure, information acquiring, formulation, dissemination and use and the public relations among them. In modern conditions, a state is faced with a complex and dynamic changing information security environment. This environment is characterized by the threats from other states, transnational terrorism and criminal networks and new technologies [2]. Such threats include information war, cyber-terrorism, cybercrime, cyber- espionage, cyber-sabotage, theft of personal information, and so forth [2, 3].

Protection of information field from modern threats is one of the priorities of national security at the moment [4]. The whole spectrum of information security threats should be monitored, timely detected and assessed, and effective measures should be taken to sustain their impact at a reasonable level. However, in practice, especially in the context of various resources, information security is achieved through the optimization of the required level of security by allowing a certain value of risk [5]. Therefore, threats should be ranked in accordance with their priorities based on assumed results, and after being structured the hierarchy of threats and corresponding responses should be developed [6].

The ranking of information security threats to e-government is crucial for taking immediate measures against these threats. Such counteraction comprises a systematic approach and the use of political, economic, organizational and technical tools. However, despite the scientific and practical significance of the issues considered, any generalized approaches to the assessment and classification of the threats have not been developed in scientific literature yet [7].

The goal of this article is to develop a methodological approach to rank the information security threats to e-government. This approach is based on multicriteria decision-making methodology [8]. In accordance with the main stages of this methodology, this paper examines the list of threats (alternatives), selection of criteria, determination of criteria weight, and threats assessment. An optimization model is proposed for the consensus ranking of threats and the experimental results are presented in numbers.

## The statement of the problem

Assume that a list of $n$ number of national cyber-security threats $A_i$ $(i = 1,2, \dots, n)$ is designed (based on official documents, scientific research, and media). Assume that $p$ number of experts $DM_k$ $(k = 1,2, \dots, p)$ are selected out of the representatives of civil society, such as scientists, who study the political, legal, economic, military, technological aspects of information security,

including the practitioners with great experience in information security, journalists, public figures, and human rights activists. Each of the experts should assess the threats in the threat list in terms of $m$ number of criteria $C_j$ $(j = 1,2, \dots, m)$. The experts highly rate potential threats, the impact of which is higher. Threat assessment is carried out on a 6-point scale: 0 - No threat; 1 - Low; 2 - Accessible; 3 - Medium; 4 – Significant; 5 - High.

Evaluation is performed by each expert, and $X^k = \left(X_{ij}^k\right)_{n\times m}$ $k = 1,2, \dots, p$ decision matrices are obtained. Each decision matrix is primarily normalized to minimize the impact of high values. Normalization is carried out according to the each criterion $j$ as follows (for simplicity, the index $k$ above the elements $x_{ij}^k$ of the further formulas is not written):

$$x_{ij} = \frac{X_{ij}}{\sum_{i=1}^{n} X_{ij}} \tag{1}$$

Based on these expert assessments, the determination of criteria weights for each expert (w ^ C = (w_1 $w^C = (w_1^C, w_2^C, \dots, w_m^C)$, alternatives assessment $(A_1' > A_2' > \cdots > A_n')$, determination of experts' weights $(w = (w_1, w_2, \dots, w_p))$ and the final consensus decision on the ranks $(r^* = (r_1, r_2, \dots, r_n))$ is required.

**National interests in the field of information and threats**

Strategic and current issues of internal and foreign policy of the state on information security are formed based on the national interests of the country in the information field. Therefore, the national interests of the country should be identified to select the criteria for defining and evaluating the information security threats of e-government. The national interests of the country in the field of information can be identified based on the official government documents (national security concept, information security concept, doctrine, relevant legislation documents). For example, Information Security Doctrine of the Russian Federation dated 2000 defines the following components of the national interests of the country in the field of information (a different list is given in the new doctrine adopted in 2016) [9]:

- ensuring freedom of information;
- protection and development of national spiritual values and traditions, cultural and scientific potential of the country;
- information provision of the state policy;
- protection of information resources from unauthorized access, ensuring security of information and telecommunication systems.

The maturity level of ICT in the countries is different, thus different categories of national interests and information threats may be identified for specific countries. However, due to the globalization, many information security problems are the identical for most countries.

E-government information security threats can be ranked at operative, tactical and strategic management levels and from the short and long term perspective. For example, cyber-security level identified by the MS-ISAC center, which indicates the current level of malicious cyber-activity and potential damage [10].

This article reviews the strategic threats. The strategic threats to the information security of e-government can result in the incidents at national level. Several key levels of strategic threats to the state can be identified from the information security point of view. Two major categories of strategic threats can be distinguished:

- Persistent threats to the information security during the given period;
- threats with greater consequences and uncertain probability - more serious threats resulting from dramatic development of current trends.

The main categories of strategic threats to the information security of e-government can also be structured in respective sub-categories.

In recent years, national cyber security strategies have been adopted in most advanced countries [12]. These strategies define the main trends of their elimination by identifying the key potential threats in latest 5-10 years and stating from the national interests of the countries in the information field. Analysis of national cyber security strategies shows that the following key categories of threats are specified in these strategies: cyber- espionage, cyber-terrorism, cyber-extremism, cyber-crime, cyber-attacks to critical infrastructure, and cyber-attacks to individual data.

As for the frequency of strategic risk assessment, note that, according to the rules of risk assessment adopted by the United Kingdom, such risks should be assessed every five years [14].

## Criteria for threats assessment

The life cycle of threat management may include the following iterative stages: potential threats identification, threats analysis, threat assessments, threat evaluation – ranking the priorities and selecting and implementing appropriate countermeasures to minimize potential impacts of the threat.

Identification of threats is an uninterrupted process, and internal and external environments covering the system are monitored continuously to define the presence of real threats. Threats are analyzed using its key components: threat actors, objectives and potential capabilities of the threat actors, targets of threat actors, vulnerabilities used by the threat, technology for implementing the threats and the consequences of threats.

Threat actors include states, terrorists (cyber or other), industrial spies, criminals, hacktivist, entertainment hackers and so forth. External and internal sources of threats to e-government information can be distinguished.

Threats are implemented through vulnerabilities (cyber-attack), which may include uninstalled software. Cyber-attacks may include Distributed denial-of-service (DDoS), cyber-espionage, and so forth.

The main factors of the threat during its assessment are the probability of the threat and the extent of its effects on the target. The probability of the threat typically depends on the potential and intent of the threat actor. Affected economic damage can be manifested in the form of financial damage, human losses, and social/structural changes. The potential impact of the threat should be measured by taking these factors into account, and should represent the level of impact of the threat on operations and strategic interests. The effects of threats to the information security of the state can be large and uncertain. However, the evaluation of these quantities in practice is challenging [16]. It is therefore more expedient to use a relative loss criterion rather than an absolute loss caused by a threat, which, in essence, characterizes the threat created by the danger to certain national interests. The relative danger of the threat to the national interest is assessed by experts on verbal indications. To assess the relative hazards of threats, multi-criteria decision-making methods based on fuzzy logic can be used [17].

## Review of related studies

### *Multi-criteria decision-making methods*

At present, researchers have proposed a large number of multi-criteria decision-making (MCDM), such as AHP (*Analytic Hierarchy Process*) [18], ANP (*Analytic Network Process*) [19], TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*) [20], VIKOR (*VIsekriterijumska Optimizacija i Kompromisno Resenje: multicriteria optimization and compromise solution*) [21], DEMATEL (*Decision-Making Trial and Evaluation Laboratory*) [22], ELECTRE II (*ELimination Et Choix Traduisant la REalité: ELimination and Choice Translating REality*) [23], PROMETHEE II (*Preference Ranking Organization METHod for Enrichment Evaluation*).

AHP was developed by Thomas Saaty (18). Its main purpose is modeling a subjective decision-making process on a hierarchical system based on a number of attributes. ANP is a summarization of AHP [19]. Normally, many decision processes cannot be structured hierarchically. The top level elements of the hierarchy may have interactions and dependencies with the low level elements. AHP does not take into account such interdependence and contradictions. ANP developed by Saaty eliminates these shortcomings.

TOPSIS, developed by Hwang C.L. and Yoon K. in 1981, is a classic approach to multi-attribute and multi-criteria decision-making issues (MADM/MCDM) [20]. The alternate is chosen which is in the closest distance from an ideal positive solution and in the furthest distance from the negative ideal solution.

VIKOR was developed for multi-criterion optimization of complex systems. It sets out compromise solutions out of alternatives for conflicting issues, which can help decision makers to reach a final decision.

DEMATEL was developed by Gabus and Fontela in 1973 [22]. This method describes factors as mutual relationships between the criteria. Therefore, DEMATEL is a complete method for constructing a structural model involving associations of complex factors. This method has been successfully applied to many different situations, such as marketing strategies development, control systems development, solution of security issues, and group decision-making.

The first outranking method was proposed by ELECTRE I Roy in 1968 [23]. Since then, its several editions have been developed (ELECTRE I, ELECTRE II, ELECTRE III, ELECTRE IV, ELECTRE IS, and ELECTRE TRI). ELECTRE II is used for ranking. ELECTRE III is an improvement of ELECTRE II, which takes into account the inaccuracies or uncertainties of data.

PROMETHEE is a ranking method developed by Brans and Vincke in the mid-1980s. Building its mathematical model is relatively easy for decision makers [24]. PROMETHEE is an improved version of ELECTRE and differs from it in the stage of peer comparison and it is easier in use.

Traditional MCDM methods are not capable to represent the ambiguities of the human judgments yet. The theory of fuzzy sets proposed by Zadeh in 1965 is widely used to model such uncertainties [25]. It also effectively overcomes uncertainties of information in multi-criterion decision-making. Evaluation of alternatives on criteria and importance weight of criteria are expressed in linguistic values [26]. The application of fuzzy approach has employed some solutions for fuzzy MCDM issues such as fuzzy AHP, fuzzy TOPSIS [27], and fuzzy VIKOR [28]. However, there is no best solution for general fuzzy MCDM. Fuzzy ranking methods have some disadvantages [28]: 1) lack of sensitivity when comparing similar fuzzy numbers; 2) in some cases, results opposing to intuition; 3) complexity of calculations. For this reason, researchers have recently attempted to combine different methods to select the best alternative [29-32].

In recent years, researchers have focused on applying multi-criteria decision-making methods in the field of information security. For example, multi-criteria decision-making methods are introduced for the threats assessment in uncertainty environment [31], information security risks assessment [32] and taking measures against them [33], and decision-making on information security risk assessment [34], and assessment of information security policy of e-government [35] and so forth.

***Rank aggregation methods***

There are different approaches to selecting the Aggregation function to combine different individual ranges in a group consensus, which is explores in [36-38] in details.

The combination of several ranking results in the consensus ranking is known as a rank aggregation [39]. Most aggregation approaches implement major voting to generate the ultimate ranking without being detected. For example, the simplest approach may calculate the median of individual ranks. Borda Counts method [40] lists the subjects based on their position and calculates the number of points scored by subjects for each voter. There are two methods of rank aggregation:

supervised and unsupervised. Most non-supervised rank aggregation methods count all the lower subjects in the list for the subject. Median Rank Aggregation [40] lists the subjects based on their ranking medians in all ranking lists. One of the fundamental shortcomings of these methods is that they have to process all their ranking in the same way. However, different systems have different accuracy and should be handled differently. Typically, supervised rank aggregation determines the weight of each ranking list by studying the aggregation function using the marked data [41]. Supervised aggregation performs high accuracy; however marked data is not always available in practice. [42] offers a model for studying the weights of the unsupervised ranking lists by optimizing the weighted Borda Count.

**The method for the determination of criteria weight based on a distance**

Traditional methods of determining the weights of criteria include expert methods, Delphi, AHP, variation coefficient method, and entropy methods [36]. The first three approaches includes subjective effects of decision makers. However, the last two approaches determines the weights without the direct participation of experts. Compared to the three previous methods, their main advantage is to eliminate the subjectivity of experts in the determination of the criteria. It is very useful when these experts do not agree on the weight values.

*Entropy-based method for criteria weight determination*. The process of calculating the weight of criteria based on entropy consists of the following steps:

a) calculation of entropy for the *j*-th criterion. Entropy value for each criterion $C_j$ is calculated as follows:

$$E_j = -k \sum_{i=1}^{n} x_{ij} log(x_{ij}) \tag{2}$$

where *k* is constant and is defined by relation $k = 1/\log(m)$ , *m* - the number of criteria.

b) Dispersion size for each criterion *Cj*. Dispersion size of the *j*-th criterion in entropy method is defined as follows:

$$\varphi_j = 1 - E_j \tag{3}$$

c) Determination of the criterion weights. Weight for each criterion *Cj* is calculated as follows:

$$w_j^C = \frac{\varphi_j}{\sum_{j=1}^{m} \varphi_j} \tag{4}$$

*The method of determining the criterion weights based on a distance*. Weight determination method based on a distance works as follows:

a) Determination of optimistic/pessimistic values for the *j*-th criteria. Optimistic and pessimistic values for each criterion $C_j$ are defined as follows:

optimistic values: $U^+ = (U_1^+, U_2^+, \dots, U_m^+)$ (5)

pessimistic values: $U^- = (U_1^-, U_2^-, \dots, U_m^-)$ (6)

Here

$$U_j^+ = \begin{cases} \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{7}$$

$$U_j^- = \begin{cases} \min\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_1, \\ \max\limits_{1 \le i \le n} \{x_{ij}\}, j \in J_2. \end{cases} \tag{8}$$

where $J_1$ describes the positives criteria (e.g. revenue), $J_2$ - negative criteria (e.g. expense).

b) Calculation of the distances between criterion values and optimistic/pessimistic values.

The distance between the values ($j$ = 1, 2, ..., $m$) of the $j$-th criterion and the optimistic/pessimistic criterion values is calculated as follows:

$$d_j^- = \sqrt{\sum_{i=1}^{n} \left(x_{ij} - U_j^-\right)^2} \tag{10}$$

c) The size of dispersion for each criterion $C_j$ is defined as follows:

$$\xi_j = \frac{d_j^+}{d_j^+ + d_j^-} \tag{11}$$

d) Calculation of the criteria weights. Based on the dispersion size, the weight of each criterion $C_j$ is determined:

$$w_j^C = \frac{\xi_j}{\sum_{j=1}^{m} \xi_j} \tag{12}$$

Once the criteria weights are determined, the decision value of the $i$–th alternative can be calculated in the following additive form:

$$z_i = \sum_{j=1}^{m} w_j^C x_{ij}, \;\; i = 1,2, \dots, n \tag{13}$$

**Optimization method for consensus ranking**

Each expert can get the final ranks of alternatives based on the values he/she gave performing the standard MCDM process. The question is the aggregation of these individual ranks in group consensus ranks [43].

The issue of weighted consensus ranking can be summarized as follows.

Assume that $r_i = (r_{i1}, r_{i2}, \dots, r_{in})$ is the ranks vector assigned to the threats by the $i$-th expert ($i$ = 1, ..., $p$), where $r_{ij}$ is the rank assigned to the $j$-th threat by the $i$-th expert ($j$ = 1 , ..., $n$). The question is to find $r^*$ weighted consensus rank of the threats by assigning the individual weight $w_i$ to each expert. The goal is to minimize the weighted distances between $r^*$ and all $r_i$. If $w = \left(w_1, w_2, \dots, w_p\right)$ is the vector of the weights assigned to the experts, then the issue of weighted consensus rabking can be expressed as the following optimization problem:

$$argmin_{\boldsymbol{w},\boldsymbol{r}^*}(1-\lambda)\sum_{i=1}^{p} w_i \|r^* - r_i\|^2 + \lambda\|w\|^2, \tag{14}$$

$$\text{Conditions: } \sum_{i=1}^{p} w_i = 1, \;\; w_i \geq 0, \forall i$$

where $0 \leq \lambda \leq 1$ is the regularization parameter, which regulates the balance between the weighted distance minimization and the smoothness of the weights. For simplicity, the Euclidean distance is used to measure the inconsistency between the consensus ranking $r^*$ and the individual expert ranking $r_i$. Therefore, $w_i\|r^* - r_i\|^2$ measures the weighted distance between the rank vector of the $i$-th expert and $r^*$ , and the first term in formula (14) is used to minimize this distance for each expert. The second sum and in formula (14) is the regulation term ensuring the smoothness of the weights.

This issue is a matter of optimizing the quadratic function with linear constraints and in [44] the following algorithm is proposed for its fast solution.

$w_i = \frac{1}{p}$ start values are given and the following two steps are repeated to solve the optimization issue:

*Step* 1: The optimal solution for $r^*$ is found by fixing $w$. Optimal solution is a weighted median:

$$r^* = \sum_{i=1}^{p} w_i r_i. \tag{15}$$

*Step* 2: The optimal solution for $w$ is found by fixing$r^*$. Assume that

$$d = \|r^* - r_1\|^2, \|r^* - r_2\|^2, \dots \|r^* - r_k\|^2 \in \mathbb{R}^p.$$

Taking into account that,

$$(1-\lambda)\sum_{i=1}^{p} w_i \|r^* - r_i\|^2 + \lambda\|w\|^2 = (1-\lambda)d^T w +$$

$$+\lambda w^T w = \lambda \left\| w - \frac{\lambda - 1}{2\lambda} d \right\|^2 - \frac{(\lambda-1)^2}{4\lambda}\|d\|^2$$

Then the optimization issue for $r^*$ with the fixation will be as follows:

$$argmin_{\boldsymbol{w}} \left\| w - \tfrac{\lambda-1}{2\lambda} d \right\|^2, \tag{16}$$

Conditions: $\sum_{i=1}^{p} w_i = 1, \;\; w_i \geq 0, \forall i.$

This is a matter of optimizing the quadratic function of the variable *p* with linear constraints (the number of variables equals to the number of experts). This problem can be solved by simply projecting the vector $\frac{\lambda-1}{2\lambda} d$ to the simplex $(p-1)$, and [45] can be addressed for an effective projection algorithm.

Steps 1 and 2 are iteratively updates while $w$ and $r^*$ are gathered. Then the weighted consensus ranking is obtained by progressively adjusting $r^*$.

Gathering: For simplicity the formula (14) is denoted as *D*, and starting values of $w$ və $r^*$- as $w_0$ and $r_0^*$. Starting with the initial values, two-step procedure is repeated: $r_i^* = argmin\, D(w_{i-1}, r_{i-1}^*)$ and $w_i = argmin\, D(w_{i-1}, r_i^*)$, where $i$ is used to denote the iteration. Hence, $D(w_i, r_i^*) \leq D(w_{i-1}, r_i^*) \leq D(w_{i-1}, r_{i-1}^*)$. Consequently, *D* is significantly diminished in each iteration and always remains positive. Thus, gathering can be achieved for this procedure most of the time.

A numerical example is provided in the following section to verify the proposed methodology.

**Experimental analysis**

This section presents an illustrative numerical example to describe the implementation process of the proposed consensus ranking method. Assume that the following five threats have been made:

- $A_1$ - cyber-espionage;
- $A_2$ - cyber-terrorism;
- $A_3$ - Cyber-crime;
- $A_4$ - cyber attacks to critical infrastructure;
- $A_5$ - cyber attacks to personal data.

Assume that three experts evaluate these threats in relation to the following criteria:

- $C_1$ - degree of violation of e-government services;
- $C_2$ - degree of damage to intellectual property;
- $C_3$ - degree of hazard to individual data.

Table 1 presents the normalized evaluation matrices based on the estimates given by each expert for these three criteria and five threats. Note that all three criteria from the viewed evaluation context are positive.

Table 1

Numerical example for multi-criteria decision-making

| Threats | $DM_1$ | | | $DM_2$ | | | $DM_3$ | | |
|---|---|---|---|---|---|---|---|---|---|
| | $C_1$ | $C_2$ | $C_3$ | $C_1$ | $C_2$ | $C_3$ | $C_1$ | $C_2$ | $C_3$ |
| $A_1$ | 0,43 | 0,43 | 0,14 | 0,23 | 0,38 | 0,39 | 0,20 | 0,50 | 0,30 |
| $A_2$ | 0,17 | 0,33 | 0,50 | 0,17 | 0,42 | 0,41 | 0,50 | 0,25 | 0,25 |
| $A_3$ | 0,29 | 0,14 | 0,57 | 0,23 | 0,38 | 0,39 | 0,27 | 0,27 | 0,46 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $A_4$ | 0,33 | 0,25 | 0,42 | 0,40 | 0,30 | 0,30 | 0,62 | 0,13 | 0,25 |
| $A_5$ | 0,45 | 0,36 | 0,18 | 0,25 | 0,33 | 0,42 | 0,10 | 0,40 | 0,50 |

Table 2 illustrates the results of determination of the weights of criteria through different methods based on the estimates given by each expert.

Table 2

Criteria weights determined by different approaches

| Expert | Criteria | Entropy-based method | | | Distance-based method | |
|---|---|---|---|---|---|---|
| | | $\varphi_j$ | $w_j^C$ | | $\xi_j$ | $w_j^C$ |
| $DM_1$ | $C_1$ | -0,4197 | 0,3548 | | 0,2437 | 0,4238 |
| | $C_2$ | -0,4110 | 0,3474 | | 0,1555 | 0,2704 |
| | $C_3$ | -0,3524 | 0,2978 | | 0,1758 | 0,3058 |
| $DM_2$ | $C_1$ | -0,4268 | 0,3174 | | 0,2437 | 0,5804 |
| | $C_2$ | -0,4587 | 0,3112 | | 0,1198 | 0,2853 |
| | $C_3$ | -0,4590 | 0,3414 | | 0,0564 | 0,1343 |
| $DM_3$ | $C_1$ | 0,3742 | 0,3618 | | 0,2679 | 0,4739 |
| | $C_2$ | 0,3394 | 0,3282 | | 0,1765 | 0,3122 |
| | $C_3$ | 0,3204 | 0,3101 | | 0,1209 | 0,2139 |

By using the criteria weights given in Table 2, threats assessment can be obtained by using the formula (13). The results are presented in Table 3.

Table 3

Decision values obtained in standard MCDM process

| Weight method | Expert | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ |
|---|---|---|---|---|---|---|
| Entropy-based method | $DM_1(z_1)$ | 0,3436 | 0,3239 | 0,3213 | 0,3290 | 0,3383 |
| | $DM_2(z_2)$ | 0,3244 | 0,3246 | 0,3244 | 0,3227 | 0,3254 |
| | $DM_3(z_3)$ | 0,3295 | 0,3405 | 0,3289 | 0,3445 | 0,3225 |
| Distance-based method | $DM_1(z_1)$ | 0,3413 | 0,3142 | 0,3351 | 0,3359 | 0,3431 |
| | $DM_2(z_2)$ | 0,2943 | 0,2736 | 0,2943 | 0,3580 | 0,2957 |
| | $DM_3(z_3)$ | 0,3151 | 0,3685 | 0,3106 | 0,3879 | 0,2792 |

As it is seen from Table 3, various experts may obtain different values for specific threats depending on the criteria weight determining method. Additionally, evaluation results may differ, even when using different techniques for finding the same expert weights. There are two types of aggregation at different levels: aggregation of decisions made by different experts and aggregation of decision results obtained by the same expert but through different weight determination method. The scenario aggregation can easily be got on Table 4 by modifying the description in Table 3.

Table 4

Assessment results through different weight determination methods

| Decision maker | Weight method | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ |
|---|---|---|---|---|---|---|
| $DM_1$ | Entropy-based method | 0,3436 | 0,3239 | 0,3213 | 0,3290 | 0,3383 |
| | Distance-based method | 0,3413 | 0,3142 | 0,3351 | 0,3359 | 0,3431 |
| $DM_2$ | Entropy-based method | 0,3244 | 0,3246 | 0,3244 | 0,3227 | 0,3254 |
| | Distance-based method | 0,2943 | 0,2736 | 0,2943 | 0,3580 | 0,2957 |
| $DM_3$ | Entropy-based method | 0,3295 | 0,3405 | 0,3289 | 0,3445 | 0,3225 |
| | Distance-based method | 0,3151 | 0,3685 | 0,3106 | 0,3879 | 0,2792 |

Table 5 summarizes the results of different weight determination methods by each expert.

Table 5

Aggregation of the results of various weight determination methods

| | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ |
|---|---|---|---|---|---|
| $DM_1$ | 0,3459 | 0,3107 | 0,3290 | 0,3336 | 0,3464 |

| | | | | | |
|---|---|---|---|---|---|
| $DM_2$ | 0,3149 | 0,3086 | 0,3149 | 0,3391 | 0,3102 |
| $DM_3$ | 0,3314 | 0,3486 | 0,3178 | 0,3535 | 0,3068 |

The next question is to combine the aggregation results by three different experts in the final decision. The main point here is to identify the experts' weights. The final decision, calculated using the experts' weights found with formula (28), is shown in Table 6.

Table 6

Final ranking obtained by the aggregation of experts' estimates

| Final decision | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ |
|---|---|---|---|---|---|
| Aggregated decision value | 0,3307 | 0,3226 | 0,3206 | 0,3421 | 0,3211 |
| Rank | 2 | 3 | 5 | 1 | 4 |

Table 6 shows that the threat $A_4$ (cyber attacks to critical infrastructure) holds the highest rank, followed by the threats $A_1$ (cyber-espionage), $A_1$ (cyber-terrorism), $A_5$ (cyber-attacks to personal data) and $A_3$ (cyber-crime). Thus, $A_4$ is the most dangerous threat out of five threats assessed by three experts on three different criteria.

## Conclusion

The list of threats to the e-government's information security is expanding, and their priorities are also changing in terms of state's response to optimally minimize the potential impacts of these threats. Now the threats in political, foreign and military spheres are becoming even more urgent, while in early 2000s, the threats were, first and foremost, of economic character. Threat ranking is a critical process for information security. It enables the identification of prioritized threats within the resources allocated to provide information security. In this study, a model was proposed for minimizing the degree of inconsistency in the evaluation of the experts, who represent political and intellectual elite, when deciding on ranking the main threats to national information security. The lack of compromise in elita's views on information security in the country is a problem and, unfortunately, it has not been studied enough. The widespread method of revealing these views is a survey questionnaire. The further studies will be on the statistical analysis of expert survey data, including cluster analysis and correlation analysis, data summarization and interpretation of results.

## References

1. Libicki M. C. Conquest in cyberspace: National security and information warfare. Cambridge University Press, 2007, 336 p.
2. European Union Agency For Network and Information Security: ENISA Threat Landscape Report 2017 (ETL 2017). January 2018, 114 p.
3. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity // Journal of Computer and System Sciences, 2014, vol.80, no.5, pp.973–993.
4. Sabillon R., Cavaller V., Cano J. National cyber security strategies: Global trends in cyberspace // International Journal of Computer Science and Software Engineering, 2016, vol.5, no.5, pp.67–81.
5. Jerman-Blažič B. An economic modelling approach to information security risk management // International Journal of Information Management, 2008, vol.28, no.5, pp.413–422.
6. Pierazzi F., Apruzzese G., Colajanni M., Guido A., Marchetti M. Scalable architecture for online prioritization of cyber threats / Proceedings of the 9th NATO International Conference on Cyber Conflicts, 2017, pp.1–22.
7. Imamverdiyev Y. Analysis of the state of the are of information security management of e-government // Information society problems, 2012, No 2 (6), pp.19–26.
8. Zavadskas E. K., Turskis Z., and Kildienė S. State of art surveys of overviews on MCDM/MADM methods //Technological and economic development of economy, 2014, vol.20, no.1, pp.165–179.

9. The Doctrine of Information Security of the Russian Federation: President of the Russian Federation 9 September. 2000. No1895.
10. Multi-State Information Sharing & Analysis Center (MSISAC). http://msisac.cisecurity.org/alert-level/
11. Lundberg R., and Willis H. H. Deliberative risk ranking to inform homeland security strategic planning // Journal of Homeland Security and Emergency Management, 2016, vol.13, no.1, pp.3–33.
12. Imamverdiyev Y.N. New generation national cyber security strategies // Information society problems, 2013, No2, pp.42–51.
13. Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication,Tallinn 2012, 253 p.
14. OECD: National Risk Assessments: A Cross Country Perspective. OECD Publishing, Paris, 2018, 308 p. http://dx.doi.org/10.1787/9789264287532-en.
15. Robinson N., Gribbon L., Horvath V., Robertson K., Cyber-security threat characterization: A rapid comparative analysis. RAND Corporation. 2013, 9 p.
16. Pochuev S.I., Bolshakov V.P. Methodological Approach to Solving the Problem of Ranking the Level of National Security Threats // Informmost, 2007, No. 6 (53), pp.34–36.
17. Changwen Q., and You H. A method of threat assessment using multiple attribute decision making / Proc. of the 6th IEEE International Conference on Signal Processing, 2002, vol.2, pp.1091–1095.
18. Saaty T.L. The analytic hierarchy process. New York: McGraw-Hill, 1980, 287 p.
19. Saaty T.L. Decision making with dependence and feedback: The analytic network process. Pittsburgh: RWS Publications, 1996, 370 p.
20. Hwang C.L. and Yoon K. Multiple attribute decision making: Methods and applications, vol.186. New York: Springer, 1981, 259 p.
21. Opricovic S. Multicriteria optimization of civil engineering systems. PhD Thesis, Faculty of Civil Engineering, Belgrade, 1998, 302 p.
22. Gabus A. and Fontela E. The DEMATEL observer. Battelle Geneva Research Center, Geneva, Switzerland, 1976.
23. Roy B. and Bertier B. La méthode ELECTRE II: une méthodede classement en presence de critèresmultiples. Note de Travail 142, Groupe Metra, Direction Scientifique, 1971.
24. Brans J. P. and Vincke P. A preference ranking organisation method: the PROMETHEE method for MCDM // Management Science, 1985, vol.31, no.6, pp.647–656.
25. Zadeh L. A. Fuzzy sets // Information and Control, 1965, vol.8, no.3, pp.338–353.
26. Buckley J. J., Feuring T., and Hayashi Y., Fuzzy hierarchical analysis revisited // European Journal of Operational Research, 2001, vol.129, no.1, pp.48–64.
27. Torfi F., Farahani R. Z., and Rezapour S. Fuzzy AHP to determine the relative weights of evaluation criteria and Fuzzy TOPSIS to rank the alternatives // Applied Soft Computing, 2010, vol.10, no.2, pp.520–528.
28. Alguliyev R. M., Aliguliyev R. M., and Mahmudova R. S. Multicriteria personnel selection by the modified fuzzy VIKOR method // The Scientific World Journal, 2015, vol.2015, Article ID 612767, pp.1–16.
29. Büyüközkan G., and Çifçi G. A novel hybrid MCDM approach based on fuzzy DEMATEL, fuzzy ANP and fuzzy TOPSIS to evaluate green suppliers // Expert Systems with Applications, vol.39, no.3, pp.3000–3011.
30. Alguliyev R. M., Aliguliyev R. M., and Mahmudova R. S. A fuzzy TOPSIS+ Worst-case model for personnel evaluation using information culture criteria // International Journal of Operations Research and Information Systems, 2016, vol.7, no.4, pp.38–66.

31. Deng Y. A Threat assessment model under uncertain environment // Mathematical Problems in Engineering, 2015, Volume 2015, Article ID 878024, 12 pages. http://dx.doi.org/10.1155/2015/878024
32. Ou Yang Y. P., Shieh H. M., Leu J. D., & Tzeng G. H. A VIKOR-based multiple criteria decision method for improving information security risk // International Journal of Information Technology & Decision Making, 2009, vol.8, no.2, pp.267–287.
33. Yang Y. P. O., Shieh H. M., & Tzeng, G. H. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment // Information Sciences, 2013, vol.232, pp.482–500.
34. Shameli-Sendi A., Shajari M., Hassanabadi M., Jabbarifar M., & Dagenais M. Fuzzy multi-criteria decision-making for information security risk assessment // The Open Cybernetics & Systemics Journal, 2012, vol.6, no.1, pp.26–37.
35. Syamsuddin I., and Hwang J. A new fuzzy MCDM framework to evaluate e-government security strategy / Proc. of the 4th International Conference on Application of Information and Communication Technologies, 2010, pp.1–5.
36. Yu L., and Lai K. K. A distance-based group decision-making methodology for multi-person multi-criteria emergency decision support // Decision Support Systems, 2011, vol.51, no.2, pp.307–315.
37. Alfares H.K., Duffuaa S.O. Determining aggregate criteria weights from criteria rankings by a group of decision makers // International Journal of Information Technology & Decision Making, 2008, vol.7, no.4, pp.769–781.
38. Cabrerizo F.J., Alonso S., Herrera-Viedma E. A consensus model for group decision making problems with unbalanced fuzzy linguistic information // International Journal of Information Technology & Decision Making, 2009, vol.8, no.1, pp.109–131.
39. Manmatha R., Rath T., and Feng F. Modeling score distributions for combining the outputs of search engines / Proc. of the 24th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, 2001, pp.267–275.
40. Van Erp M., and Schomaker L. Variants of the Borda count method for combining ranked classifier hypotheses / Proc. of the 7th International Workshop on Frontiers in Handwriting Recognition, 2000, pp.443–452.
41. Liu Y.-T., Liu T.-Y., Qin T., Ma Z.-M., and Li H. Supervised rank aggregation / Proc.of the 16th International Conference on World Wide Web, 2007, pp.481–490.
42. Klementiev A., Roth D., and Small K. An unsupervised learning algorithm for rank aggregation / Proc. of the European Conference on Machine Learning, 2007, pp. 616–623.
43. Imamverdiyev Y. N. Consensus ranking method of information security threats of a nation state / II Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", 2017, pp.12–13.
44. Wang D., and Li T. Weighted consensus multi-document summarization // Information Processing & Management, 2012, vol.48, no.3, pp.513-523.
45. Duchi J., Shalev-Shwartz S., Singer Y., and Chandra T. Efficient projections onto the $l_1$-ball for learning in high dimensions / Proc. of the 25th International Conference on Machine Learning, 2008, pp.272–279.