I. J. Computer Network and Information Security, **2024, 1, 24-34**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.01.02

Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory

Oleksandr Evgeniyovych Korystin*
State Scientifically Research Institute of the MIA of Ukraine, Kyiv, Ukraine
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
E-mail: alex@korystin.pro
*Corresponding Author

Oleksandr Korchenko
University of the National Education Commission, Cracow, Poland
National Aviation University, Kyiv, Ukraine
E-mail: agkorchenko@gmail.com

Svitlana Kazmirchuk
National Aviation University, Kyiv, Ukraine
E-mail: sv.kazmirchuk@gmail.com

Serhii Demediuk
National Security and Defense Council of Ukraine, Kyiv, Ukraine
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
E-mail: cyberdemediuk@protonmail.com

Oleksandr Oleksandrovych Korystin
National Aviation University, Kyiv, Ukraine
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
E-mail: alexkorystin@ukr.net

Received: 09 January 2023; Revised: 18 March 2023; Accepted: 27 April 2023; Published: 08 February 2024

Abstract: Applied results of scientific analysis should be the key focus of modern security research. A comparative analysis of research results obtained using different methods, as an applied task, forms a broader basis for interpreting the results and substantiating the conclusions. A social survey and expert opinion research were conducted to implement the general concept of strategic analysis of cybersecurity in Ukraine. Using the method based on determining the average value in a certain set of estimates, as well as the method based on the theory of fuzzy sets, the risks of spreading certain cyber threats in Ukraine were assessed. The results were compared. Although the use of different measurement methods led to some differences in quantitative risk indicators, the comparative analysis of the ratio of the level of different cyber threats did not change significantly. At the same time, the fuzzy set method provided more flexible interpretation of the results to characterize cyber threats in terms of their upward or downward trend. In general, the combined approach to cyber threat risk assessment can become an important risk management tool, as it takes advantage of different methods and allows for a deeper understanding of the current situation and the formation of more informed management decisions.

Index Terms: Cybersecurity, Cyber Threats, Risk Assessment, Information Security, Fuzzy Logic, Fuzzy Set, Critical Infrastructures.

1. Introduction

Based on sociological theory (Ulrich Beck), the information society is a risk society, in which there are threats of different content and nature, as well as the distribution of risks caused by them [1]. That is why modern security management requires a new level of thinking, based on an adequate perception of risk and its key role in the methodology of understanding the security environment, predicting the future and making informed management decisions. Currently, the key focus of modern security studies should be on the applied results of scientific analysis, based on empirical research confirmation of the hypotheses put forward, focusing on existing problems, key threats and raising awareness of both society as a whole and security actors [2].

Among other things, a comparative analysis of research results obtained using different methods, as an applied task, forms a broader basis for interpreting the results and substantiating the conclusions. In this context, a comparative analysis of the application of different methods of analyzing and assessing the of cyber threats' spreading, such as methods based on determining the average value in a certain set of estimates and based on the fuzzy sets' theory, forms clarifying elements, characteristics, takes into account certain ambiguities, and the comparison of the results provides justification for the conclusions regarding the trends in the spread of cyber threats and their priority in risk management.

2. Related Works

Many researchers from different fields are involved in cybersecurity issues. Their research interests include both the development of theoretical models and the formation of appropriate methodologies, as well as applied research interests with specific security aspects. Many works are devoted to the issues of information security management, its various directions: risk management in the information security system [3-8]; information resources management in the security system [3, 9, 10]; information security management efficiency [9-11]. Particular attention is focused on identifying cybersecurity system vulnerabilities, in particular software products, and their classification [12-16]. The focus is on protecting information based on risk analysis and localization of anomalies, with an emphasis on statistical methods of detecting them [17-22]. As for the study of cyber threats, methods are applied that are grouped on quantitative and qualitative analysis [23] using an anomaly detection and intrusion detection system [24, 25], risk forecasting of data confidentiality breach [26], assess and compare the vulnerability risk of operating systems [27], intelligent recognition of anomalies and cyberattacks using logical procedures [28], and methods based on fuzzy sets [29-34].

An important study was conducted by scientists and experts at the initiative of ENISA (*European Union Agency for Cybersecurity*) on expert evaluation [35], systematization of risk management frameworks and methodologies [35, 36], where all known methodologies and systems of cyber security risk management are analyzed [37-39], their interoperability and prospective application are determined [40].

The use of common methodological approaches, modern risk management methods, risk-based ranking and relevant international standards [30, 32, 33] determined the author's approach to the methodology for further analysis and assessment of the risks of cyber threats [31] and the analysis of existing approaches to assessing information security risks [29-31], cyber security [32], security models [33], vulnerabilities of information systems [34], which are based on the use of the theory of fuzzy sets, made it possible to choose an alternative approach for further comparative analysis of the obtained results with the same input parameters.

3. Proposed Methods

3.1. Data Collection and Cleaning

To deepen the cognitive process of cybersecurity in Ukraine, a social survey and expert opinion research was conducted to implement the general concept of strategic analysis of cybersecurity in Ukraine [41]. The selected expert sample ensured a professional approach and professional awareness of the survey subject. The developed questionnaires were filled out in anonymous and confidential mode in ON-LINE, in which each indicator was evaluated by two characteristics: «Likelyhood» and «Consequences».

In order to extract the most reliable information from the data obtained, providing statistical justification for the sample limitation procedure [42, 43], questionnaires were selected only from those experts who provided logically consistent answers.

3.2. Risk Assessment

The methodological basis for the initial stage of the analysis is the ISO 31000 recommendations [44], while the author's approach to data structure, assessment grading, and integration of cyber threat assessment characteristics is unique: Likelyhood and Consequences [45].

The following assessment of cyber threats is presented in Table 1, where, based on the average Likelihood of their spread, they were assessed on a scale: low - 0; medium - 5; high - 10, and Consequences on a scale: minor consequences - 0; severe - 5; critical - 10; catastrophe - 15.

Further analysis was carried out using IBM SPSS Statistics software. Based on the syntax [45, 46], the integrated value of the risk assessment of the spread of threats and presented as a percentage on a scale from 0 to 100% (Table 2). Thus, a rating of cyber threats is formed by risk level.

3.3. Risk Assessment on the Qualitative-quantitative Method

To obtain an alternative risk assessment from the values of the values of "Consequences" (*PC)* and "Likelihood" *(L)* of the occurrence of a cyber threat (see Table 1), we use the qualitative and quantitative risk assessment method proposed in [29]. To process the results from Table 1, the existing method from [29] was modified by applying the fuzzification procedure using the interval transformation method [47]. This made it possible to display the field of expert judgment intervals in fuzzy numbers (FN). This interpretation of the expert's judgments with the help of FN is more natural for reflecting his opinion, in contrast to the previously used point values (ordinary numbers).

Table 1. Results of the cyber threat analysis

№	Indicator	Likelyhood	Consequences
1.	Use of cyber operations:	8,38	7,98
1.1	Cyberattack against central executive bodies (CEBs)	8,36	8,17
1.2	Cyberattack against critical infrastructure facilities	8,22	8,71
1.3	DDos attacks - distributed cyber attacks	8,12	7,78
1.4	Use of software products for covert information gathering	8,56	7,48
1.5	Interference in the electoral system	7,97	8,26
1.6	Unauthorized access to private and proprietary information arrays	8,24	7,14
1.7	Attacks or interference with state public registers (e.g., property rights, etc.)	7,66	7,2
2.	Using phishing web resources to collect information	7,9	6,31
3.	Use of Bot-net to control computers of the internal network infrastructure	7,41	6,72

Table 2. Risks assessment of cyberthreats

№	Indicator	RISK, %
1.	Use of cyber operations:	49,29
1.1	Cyberattack against central executive bodies (CEBs)	**50,03**
1.2	Cyberattack against critical infrastructure facilities	**52,25**
1.3	DDos attacks - distributed cyber attacks	46,88
1.4	Use of software products for covert information gathering	47,36
1.5	Interference in the electoral system	49,36
1.6	Unauthorized access to private and proprietary information arrays	44,03
1.7	Attacks or interference with state public registers (e.g., property rights, etc.)	42,58
2.	Using phishing web resources to collect information	38,51
3.	Use of Bot-net to control computers of the internal network infrastructure	39,03

Thus, in step 1 (Determining the full set of identifiers of information systems resources (ISR) and threats) and 2 (Determining the set of identifiers of ISR and threats for the object of evaluation) of the method, the set of ISR and threats was determined (see Table 1). In step 3 (Determining the set of risk assessment parameters), we determine the set of parameters EP_i $\left(i = \overline{1, g}\right)$, used for further evaluation, i.e.:

$$\boldsymbol{EP} = \left\{\cup_{i=1}^{g} EP_i \right\} = \left\{EP_1,\ EP_2, \dots,\ EP_g\right\},$$

where g is the number of sets of such parameters (with g=2, we get $\boldsymbol{EP}$**=** **{**PC, L**}**). Where PC is the data from Table 1 – “Consequences” and L is “Likelihood” respectively.

In steps 4 (Determining the number of term-sets), 5 (Assessing the level of significance of the evaluation parameters), 6 (Determining the reference values of the risk level), 7 (Determining the reference values of the evaluation parameters), we obtain the number of necessary term-sets for risk assessment and enter all the necessary linguistic variables (LV) that will be involved in the specified assessment process.

Taking into account the scales used to obtain the results in Table 1 and the approach in [47] is proposed to measure PC and L using point scales in the range $[c_1; c_{n+1}]$ = [0; 15] and $[l_1; l_{m+1}] = [0; 10]$, which will be displayed in intervals, respectively:

$$[c_1; c_2[, \dots, [c_i; c_{i+1}[, \dots, [c_n; c_{n+1}]$$

and

$$[l_1; l_2[, \dots, [l_j; l_{j+1}[, \dots, [l_m; l_{m+1}],$$

where c_i $(i = \overline{1, n})$ and l_j $(j = \overline{1, m})$ the corresponding numerical values of the intervals for PC and L.

For example, at n= 4 and m= 3 scales for measuring PC and L are presented as follows:

$$[c_1; c_2[, [c_2; c_3[, [c_3; c_4[, [c_4; c_5] = [0; 3[, [3; 7{,}5[, [7{,}5; 12{,}5[, [12{,}5; 15]$$

and

$$[l_1; l_2[, [l_2; l_3[, [l_3; l_4] = [0; 3[, [3; 7{,}5[, [7{,}5; 10].$$

The practice of solving problems in the field of information and cybersecurity [47, 48] has shown that it is most effective to use the theory of fuzzy sets to process expert data. In this regard, we introduced the LVs "CONSEQUENCES" (***PC***) and "LIKELYHOOD" (***L***)**.** Thus, LV ***PC*** is represented by the tuple [29] <***PC***, $\underset{\sim}{T}_{PC}$, X_{PC}>, and LV ***L*** – <***L***, $\underset{\sim}{T}_L$, X_L>, $\underset{\sim}{T}$ where the basic term sets are defined by *n* and *m* terms, respectively. For each term

$$\underset{\sim}{T}_{PC} = \cup_{i=1}^{n} \underset{\sim}{T}_{iPC}$$

and

$$\underset{\sim}{T}_{L} = \cup_{j=1}^{m} \underset{\sim}{T}_{jL}$$

accordingly, a different value interval is set $[c_1; c_2[, \ldots, [c_i; c_{i+1}[, \ldots, [c_n; c_{n+1}]$ and $[l_1; l_2[, \ldots, [l_j; l_{j+1}[, \ldots, [l_m; l_{m+1}]$.

To convert the specified intervals to fuzzy numbers FN for LV ***PC*** and ***L***, we use the interval phasing method from [47], which consists of 5 stages. For example, at stage 1 for ***PC***, the expert determined the coefficient of interval proximity $CF=0.25$. Next, let's determine the medians of the intervals when n=4, using formula (1) [47] of the second stage of this method: $M_1 = (c_2 - c_1) / 2$ =(3-0) / 2 = 1,5; M_2=5,25; M_3=10; M_4=13,75.

Next, in step 3, we calculate the shift parameter using formula (2) [47]:

$$SP = M_1 - CF(c_2 - c_1) = 1{,}5 - 0{,}25(3-0) = 0{,}75.$$

Next, at step 4, the tensile coefficient is determined using formula (3) [47]: $SC = \frac{c_5}{M_4 - CF(c_5 - c_4) - SP}$ =15/(13,75-0,25(15-12,5)-0,75) = 1,1.

At step 5, we generate the FN standards for LV ***PC*** using formulas (4-7) [47]:

$$b_{11}^{c} = SC(M_1 - CF(c_2 - c_1) - SP) = 0;\ b_{21}^{c} = SC(M_1 + CF(c_2 - c_1) - SP) = 1{,}65 \text{ etc.}$$

$$a_1 = 0;\ a_2 = b_{21} = 1{,}65;\ a_3 = 6{,}19;\ a_4 = 11{,}56;$$

$$c_1 = b_{12} = 3{,}72;\ c_2 = 8{,}81;\ c_3 = 13{,}62;\ c_4 = 15,$$

where a_i, b_{1i}, b_{2i}, c_i ($i = \overline{1, n}$, n – number of terms) abscissa of the lower and upper bases of the trapezoidal FN for LV ***PC***.

After the conversion, we get the following term values for LV ***PC*** at n=4:

$$\underset{\sim}{T}_{PC} = \cup_{i=1}^{4} \underset{\sim}{T}_{iPC} = \{\underset{\sim}{T}_{1PC} = (0; 0; 1{,}65; 3{,}72)_{LR}, \underset{\sim}{T}_{2PC} = (1{,}65; 3{,}72; 6{,}19; 8{,}81)_{LR}, \underset{\sim}{T}_{3PC} = (6{,}19; 8{,}81; 11{,}56; 13{,}62)_{LR}, \underset{\sim}{T}_{4PC} = (11{,}56; 13{,}62; 15; 15)_{LR}\}.$$

The graphical interpretation of the generated FN $\underset{\sim}{T}_{c}^{(4)}$ for LV ***PC*** is shown in Fig. 1.

Next, we implement similar transformations of intervals into FNs using the method [47] for LV ***L*****.** Suppose that the expert also chose the coefficient of proximity of intervals with the value CF=0,25. Next, we determine the medians of the intervals at m=3, by formula (1) [47] of the second stage of the above method: $M_1 = (l_2 - l_1)/2$ = 1,5; M_2=5,25; M_3=8,75.

After that, we determine the shift parameter using formula (2) [47]:

$$SP = M_1 - CF(l_2 - l_1) = 0{,}75;$$

Next, using formula (3) [47], we calculate the stretching factor: $SC = \frac{l_5}{M_4 - CF(l_5 - l_4) - SP}$ = 1,16.

And then, we form the standards FN for LV ***L*** using formulas (4-7) [47]:

$$b_{11} = SC(M_1 - CF(l_2 - l_1) - SP) = 0;\ b_{21} = SC(M_1 + CF(l_2 - l_1) - SP) = 1{,}74 \text{ etc.}$$

$$a_1 = 0;\ a_2 = b_{21} = 1{,}74;\ a_3 = 6{,}52;$$

$$c_1 = b_{12} = 3{,}91;\ c_2 = 8{,}55;\ c_3 = 10,$$

where a_j, b_{1j} , b_{2j}, c_j ($j = \overline{1, m}$, m – number of terms) the abscissa of the lower and upper bases of the trapezoidal FN for LV ***L***.

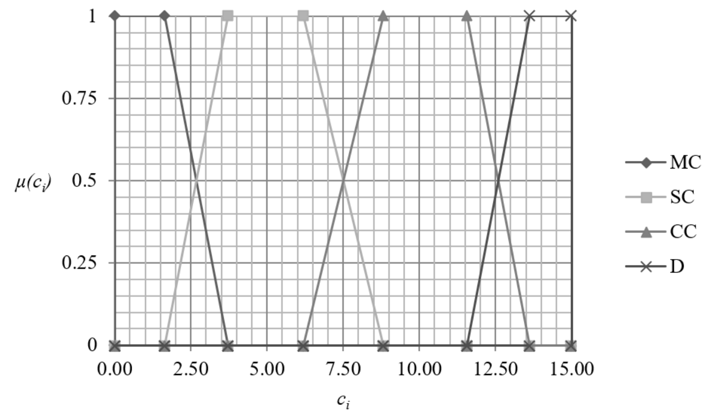

Fig.1. The terms of the values of the generated FN for LV *PC* $\underset{\sim}{T}{}_{c}^{(4)}$, where MC – minor consequences, SC – serious condition, CC – critical condition, D – disaster

After the conversion, we get the following term values for LV ***L*** at m=3:

$$\underset{\sim}{T}_{L} = \cup_{j=1}^{3} \underset{\sim}{T}_{j_L} = \{\underset{\sim}{T}_{1L} = (0; 0; 1{,}74; 3{,}91)_{LR}, \underset{\sim}{T}_{2L} = (1{,}74; 3{,}91; 6{,}52; 8{,}55)_{LR}, \underset{\sim}{T}_{3L} = (6{,}52; 8{,}55; 10; 10)_{LR}\}.$$

Graphical interpretation of the generated FN $\underset{\sim}{T}{}_{l}^{(3)}$ for LV ***L*** is shown in Fig. 2.

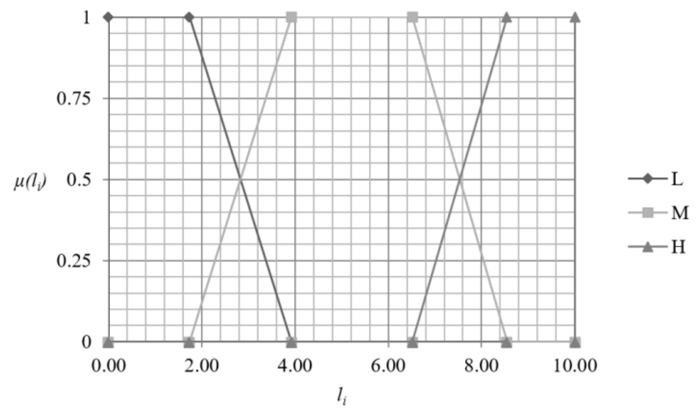

Fig.2. Terms of the values of the generated FN for LV *L* $\underset{\sim}{T}{}_{l}^{(3)}$, where L – low, M – medium, H – high

Next, by analogy, we implement the phasing of the intervals for the value «Risk level» (*RL*) and, for example, to evaluate it, we introduce LV "RISK LEVEL" (***RL***), define by a tuple [29] <***RL***, $\underset{\sim}{T}_{RL}$, X_{RL}>, where the base term set is formed on the basis of *n* terms. For each term

$$\underset{\sim}{T}_{RL} = \cup_{i=1}^{n} \underset{\sim}{T}_{iRL},$$

respectively, it is set its own interval of values, the scale of which lies within [r_1; r_{n+1}] = [0; 100], which are divided into intervals [r_1; r_2[, …, [r_i; r_{i+1}[,…, [r_n; r_{n+1}], for example, at n = 4 for ***RL*** define the following intervals**:**[r_1; r_2[, [r_2; r_3[, [r_3; r_4[, [r_4; r_5] = [0; 30[, [30; 37[, [37; 64[, [64; 100].

Next, using the method from [47], we implement the corresponding transformations of the LV ***RL*** intervals into FN, after which we obtain the following term values

$$\underset{\sim}{T}_{RL} = \cup_{i=1}^{4} \underset{\sim}{T}_{iRL} = \{\underset{\sim}{T}_{1RL} = (0; 0; 17{,}96; 29{,}04)_{LR}, \underset{\sim}{T}_{2RL} = (17{,}96; 29{,}04; 33{,}23; 43{,}41)_{LR}, \underset{\sim}{T}_{3RL} = (33{,}23; 43{,}41; 59{,}58; 78{,}44)_{LR}, \underset{\sim}{T}_{4RL} = (59{,}58; 78{,}44; 100; 100)_{LR}\}.$$

The graphical interpretation of the generated FN $\underset{\sim}{T}{}_{r}^{(4)}$ for LV ***RL*** is shown in Fig. 3.

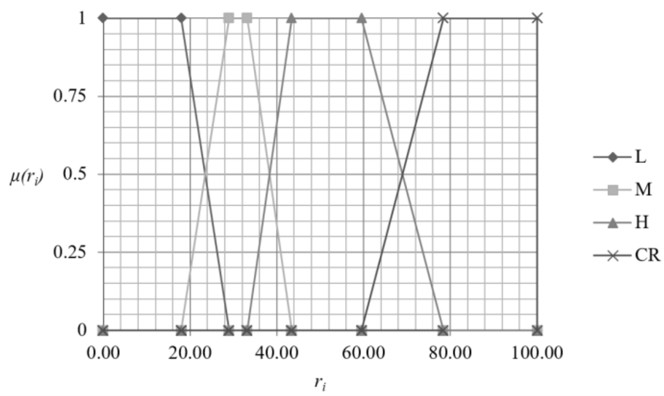

Fig.3. The terms of the values of the generated FN for LV $RL\ \underset{\sim}{T}{}_r^{(4)}$, where L – low, M – medium, H – high, CR – critical

To implement step 8 (Estimation of current parameter values) of the method [29], namely, to determine the current values of the estimated parameters

$$\left\{\cup_{\boldsymbol{i=1}}^{\boldsymbol{2}} EP_i\ \right\} = \{EP_1,\ EP_2\} = \{L, PC\}\left(i = \overline{1,2}\right),$$

experts in the relevant subject area determine $ep_{uz,i}$ $(uz = \overline{1,n},\ i = \overline{1,g}$, where g – is the number of estimated parameters, and n — number of threats) for all threats Vuz $(uz = \overline{1,n})$, that is

$$\left\{ep_{uz,i}\right\} = \{ep_{uz,L}, ep_{uz,PC}\},$$

where for the obtained values $ep_{uz,i}$ let's use Table 1. In step 9 (Classification of current values), we implement the classification of the current values of the estimated parameters ***L*** and ***PC***, by the formula [29]:

L:

$$\mu_1\left(ep_{uz,L}\right) = \begin{cases} L\left(\dfrac{a_1 - ep_{uz,L}}{a_1 - b_{11}}\right), ep_{uz,L} \in [a_1, b_{11}]; \\ 1, \qquad\qquad\qquad ep_{uz,L} \in [b_{11}, b_{21}]; \\ R\left(\dfrac{ep_{uz,L} - c_1}{b_{21} - c_1}\right), ep_{uz,L} \in [b_{21}, c_1], \end{cases}$$

$$\mu_2\left(ep_{uz,L}\right) = \begin{cases} L\left(\dfrac{a_2 - ep_{uz,L}}{a_2 - b_{12}}\right), ep_{uz,L} \in [a_2, b_{12}]; \\ 1, \qquad\qquad\qquad ep_{uz,L} \in [b_{12}, b_{22}]; \\ R\left(\dfrac{ep_{uz,L} - c_2}{b_{22} - c_2}\right), ep_{uz,L} \in [b_{22}, c_2], \end{cases}$$

$$\mu_3\left(ep_{uz,L}\right) = \begin{cases} L\left(\dfrac{a_3 - ep_{uz,L}}{a_3 - b_{13}}\right), ep_{uz,L} \in [a_3, b_{13}]; \\ 1, \qquad\qquad\qquad ep_{uz,L} \in [b_{13}, b_{23}]; \\ R\left(\dfrac{ep_{uz,L} - c_3}{b_{23} - c_3}\right), ep_{uz,L} \in [b_{23}, c_3], \end{cases}$$

PC:

$$\mu_1\left(ep_{uz,PC}\right) = \begin{cases} L\left(\dfrac{a_1 - ep_{uz,PC}}{a_1 - b_{11}}\right), ep_{uz,PC} \in [a_1, b_{11}]; \\ 1, \qquad\qquad\qquad ep_{uz,PC} \in [b_{11}, b_{21}]; \\ R\left(\dfrac{ep_{uz,PC} - c_1}{b_{21} - c_1}\right), ep_{uz,PC} \in [b_{21}, c_1], \end{cases}$$

$$\mu_2\left(ep_{uz,PC}\right) = \begin{cases} L\left(\dfrac{a_2 - ep_{uz,PC}}{a_2 - b_{12}}\right), ep_{uz,PC} \in [a_2, b_{12}]; \\ 1, \qquad\qquad\qquad ep_{uz,PC} \in [b_{12}, b_{22}]; \\ R\left(\dfrac{ep_{uz,PC} - c_2}{b_{22} - c_2}\right), ep_{uz,PC} \in [b_{22}, c_2], \end{cases}$$

$$\mu_3\left(ep_{uz,PC}\right) = \begin{cases} L\left(\dfrac{a_3 - ep_{uz,PC}}{a_3 - b_{13}}\right), ep_{uz,PC} \in [a_3, b_{13}]; \\ 1, \qquad\qquad\qquad ep_{uz,PC} \in [b_{13}, b_{23}]; \\ R\left(\dfrac{ep_{uz,PC} - c_3}{b_{23} - c_3}\right), ep_{uz,PC} \in [b_{23}, c_3], \end{cases}$$

$$\mu_4\left(ep_{uz,PC}\right) = \begin{cases} L\left(\dfrac{a_4 - ep_{uz,PC}}{a_4 - b_{14}}\right), ep_{uz,PC} \in [a_4, b_{14}]; \\ 1, \qquad\qquad\qquad ep_{uz,PC} \in [b_{14}, b_{24}]; \\ R\left(\dfrac{ep_{uz,PC} - c_4}{b_{24} - c_4}\right), ep_{uz,PC} \in [b_{24}, c_4]. \end{cases}$$

The results of the calculation are presented in Table 3.

In step 10 (Risk Assessment), we calculate the risk level indicator of information security breach using the formula [29]:

$$RL_{uz} = \sum_{j=1}^{m}\left(K_{lr_j}\sum_{i=1}^{g}(ks \cdot LS_i)\lambda_{uz,ij}\right),$$

where K_{lr_j} = 90 – 20(m – j), $ks = \frac{1}{(LS_1+\cdots+LS_i)}$ – rationing factor, $\lambda_{uz,ij}$ $(uz = \overline{1,n},\ i = \overline{1,g}, j = \overline{1,m},)$ is determined by expression (4.20) [29] for each V_{uz} $\left(uz = \overline{1,n}\right)$, and LS_i, $\left(i = \overline{1,g}\right)$ depending on the significance of the parameter is calculated by formula (4.13) or (4.14) [29]. The results are summarized in Table 4. In step 11 (Formation of the structured risk parameter), by analogy with step 8, we will classify the results obtained by the expression

$$\mu_j(RL_{uz}) = \begin{cases} L\left(\frac{a_j - RL_{uz}}{a_j - b_{1j}}\right), RL_{uz} \in [a_j, b_{1j}]; \\ 1, \qquad RL_{uz} \in [b_{1j}, b_{2j}]; \\ R\left(\frac{RL_{uz} - c_j}{b_{2j} - c_j}\right), RL_{uz} \in \left[b_{2j}, c_j\right], \end{cases}$$

and display them in Table 4. Next, according to expression (4.23) [29], we will form a structural parameter, where, for example, $SP_1 = (RL_1;\ \underset{\sim}{T}_{3RL}\ \mu_3(RL_1));\ \underset{\sim}{T}_{4RL}\ (\mu_4(RL_1)))$ = (76,15; H(0,1); CR(0,9)), which is verbally interpreted as - "The risk level with a numerical equivalent of 76,15 borders on high and critical risks on the border H – 0,1 and CR – 0,9».

Table 3. Classification of current values of evaluation parameters

№	Indicator	EP_i	***L*** **0/10** (i=1)	λ_{ij} for $\underset{\sim}{T}_{2L}$ – «M» $(i = \overline{1,2}, j = \overline{1,3})$	λ_{ij} for $\underset{\sim}{T}_{3L}$ – «H» $(i = \overline{1,2}, j = \overline{1,3})$	***PC*** **0/15** (i=2)	λ_{ij} for $\underset{\sim}{T}_{2PC}$ – «SC» $(i = \overline{1,2}, j = \overline{1,4})$	λ_{ij} for $\underset{\sim}{T}_{3PC}$ – «CC» $(i = \overline{1,2}, j = \overline{1,4})$
1.	Use of cyber operations:	$ep_{1,i}$	8,38	0,1	0,9	7,98	0,3	0,7
1.1	Cyberattack against central executive bodies (CEBs)	$ep_{2,i}$	8,36	0,1	0,9	8,17	0,2	0,8
1.2	Cyberattack against critical infrastructure facilities	$ep_{3,i}$	8,22	0,2	0,8	8,71	0,0	1,0
1.3	DDos attacks - distributed cyber attacks	$ep_{4,i}$	8,12	0,2	0,8	7,78	0,4	0,6
1.4	Use of software products for covert information gathering	$ep_{5,i}$	8,56	0,0	1,0	7,48	0,5	0,5
1.5	Interference in the electoral system	$ep_{6,i}$	7,97	0,3	0,7	8,26	0,2	0,8
1.6	Unauthorized access to private and proprietary information arrays	$ep_{7,i}$	8,24	0,2	0,8	7,14	0,6	0,4
1.7	Attacks or interference with state public registers (e.g., property rights, etc.)	$ep_{8,i}$	7,66	0,4	0,6	7,2	0,6	0,4
2.	Using phishing web resources to collect information	$ep_{9,i}$	7,9	0,3	0,7	6,31	1,0	0,0
3.	Use of Bot-net to control computers of the internal network infrastructure	$ep_{10,i}$	7,41	0,6	0,4	6,72	0,8	0,2

Table 4. Results of the risk assessment

№	Indicator	RL_{uz}	$\underset{\sim}{T}_{3RL}$ –«H»	$\underset{\sim}{T}_{4RL}$ – «CR»
1.	Using cyber operations:	76,15	0,1	0,9
1.1	Cyberattack against central executive bodies	**77,5**	**0,0**	**1,0**
1.2	Cyberattack against critical infrastructure facilities	**78,4**	**0,0**	**1,0**
1.3	DDos attacks- distributed cyber attacks	71,02	0,4	0,6
1.4	Use of software products for covert information gathering	75,25	0,2	0,8
1.5	Interference in the electoral system	72,1	0,3	0,7
1.6	Unauthorized access to private and official information arrays	70,3	0,4	0,6
1.7	Attacks or interference with state public registers (e.g., property rights, etc.)	63,1	0,8	0,2
2.	Using phishing web resources to collect information	59,5	1,0	0,0
3.	Use of Bot-net to control computers of the internal network infrastructure	56,8	1,0	0,0

4. Results and Analysis

The first methodology provides a general approach to risk assessment that is based on defined averages for assessing the relevant threats (in percentages). It makes it possible to make comparisons based on numerical data and determine which risks are greater or lesser, and provides averaged estimates, the results of which are focused on obtaining primary, simple results for comparison. Thus, the highest risk is characterized by the threats of "cyberattack against critical infrastructure facilities" (52,25%) and "cyberattack against central executive bodies" (52,03%). These results, based on average values, make it possible to compare them in terms of risk with other cyber threats that are rated below 50 percent.

In contrast to the known methods [35-40], the proposed approach [45, 46] allows to implement the process of assessing the risks of cyber threats based on the average value, and the modification of the closest theoretical solution [29] using the interval fuzzification method [47] allows obtaining a qualitatively new alternative an approach based on the theory of fuzzy sets, taking into account the nature of the expert's judgments and obtaining risk assessments based on the formed degrees of belonging to different levels. The use of fuzzy logic to implement the assessment allows for a more detailed and flexible approach to identifying preferences within the limits of changing levels of the assessment scale, for example, between the levels of "high" and "critical" ("H" and "CR") and taking into account not only numerical risk values but also membership functions indicating the degree to which an object belongs to a certain risk level. Thus, despite the fact that the absolute risk values are somewhat higher based on the alternative approach, the general trend in the ratio of the level of risk of the spread of cyber threats has remained unchanged, and this is understandable given the use of a common empirical basis. At the same time, the alternative method based on fuzzy set theory adds new aspects and characteristics to the definition of cyber threats, namely: it allows to take into account ambiguity (fuzziness) in the results, which leads to a more flexible and adaptive risk assessment; it allows to identify new important aspects of threats that may be lost in models based on average values, for example, taking into account uncertainty at the boundary values of scales when measuring various parameters; it allows to model fuzzy relationships between different elements of the system and obtain an updated risk assessment.

In practice, there are situations when valuation using statistical methods can lead to inaccuracies because, when generating such data, the expert operates in certain intervals with clearly defined boundary values that characterize the state of the object of valuation, and their averaging is reduced to a point value on a certain interval, which leads to a rough valuation. In fact, the method based on fuzzy sets allows the entire interval to be used in the assessment, taking into account the personal preferences of the expert in forming judgments.

If we use the scale for assessing the risk of threats spreading in [45], then, for example, a risk level of 50,01% (red level) refers to the most significant threats and requires urgent measures to reduce it, while a value of 50% (orange level) refers to significant threats and only requires control by top management. Logically, these figures are almost identical (the difference can be interpreted as an error) and, in fact, require the same approach to response. And given that these results are the processing of expert judgments, which are usually qualitative (fuzzy) rather than quantitative (numerical) in nature regarding assessments of a particular state of an object, the boundary between risk levels on the measurement scale is blurred. Taking into account the established FN $\underset{\sim}{T}_r^{(4)}$ for LV $\boldsymbol{RL}$ (Fig. 3) and [29], the scale for measuring the risks of threats will look like this: $\boldsymbol{RL} \in [0; 30]$ – green level; $\boldsymbol{RL} \in [30; 37]$ – yellow level; $\boldsymbol{RL} \in [37; 64]$ – orange level; $\boldsymbol{RL} \in [64; 100]$ – red level. Thus, the red level includes not only positions 1.1 and 1.2, but also 1.3÷1.6, but the first two positions, as in the calculations in [35], are dominant (the limit for «CR» >0,8), that are correlated with each other. In the alternative method, the red level, for example, includes positions 1.3÷1.5, but on the border «CR» they are characterized by values that lie in the range of [0,6; 0,8] and, if necessary, such risks can be processed to reduce their level. For item 1.6, the risk level borders on «H» – 0,4 i «CR» – 0,6 and, with limited resources, it can be put under the control of senior management and, under further favorable conditions, prioritized for processing.

Thus, the effectiveness of the proposed method, unlike the known ones, lies in the fact that it gives cyber security specialists a new opportunity with the help of fuzzy logic to make more informed decisions and develop effective risk minimization strategies based on new alternative data obtained. Such an approach can serve as a basis for the implementation of further security measures and crisis management planning.

5. Conclusions

An alternative method takes into account the nature of expert assessment based on the judgment of specialists in the relevant subject area and makes it possible to reflect risk characteristics with additional indicators of belonging to a certain level.

This, in contrast to the method based on average values [45], due to the implementation of the fuzzification procedure, allows reducing the sensitivity to threshold values in risk measurement scales and assigning almost identical values, for example, 50% and 50,01% to different levels, which leaves out of consideration the taking of urgent measures to reduce the risk of the spread of threats according to certain indicators. Also, in contrast to [45], in the alternative approach, the classification of indicators by levels does not have a jump-like nature (this can be seen in the graphic interpretation in Fig. 1, Fig. 2, and Fig. 3) and enables smooth ranking and, in the final version, a more effective distribution resources to reduce risks, rather than spending them on one resource and leaving another, which is characterized by almost the same level, untreated. This was determined in the process of a series of specific calculations when solving practical problems of assessing the risks of cyber threats.

Using alternative approaches to risk assessment can yield different results depending on which aspects of risk are important. The use of membership functions and fuzzy logic allows for a more sophisticated risk analysis and allows for the consideration of the degree to which risks belong to different levels, which can be useful for a more accurate threat assessment. It is important to take into account both approaches and use them in combination to obtain integrated information about cybersecurity risks and additional opportunities to develop effective strategies for managing them.

The analysis of the results indicates that both approaches have their advantages and the application depends on the specific situation and the objectives of the risk assessment. The first approach with numerical risk values allows for a quick comparison and determination of their overall level. However, it is not informative in terms of determining the degree of belonging to different risk levels on the scales chosen for measurement.

An alternative approach based on membership functions and fuzzy logic provides more flexibility and detail in the assessment, allowing for the level of impact of threats and the degree of belonging to different risk levels. It is especially useful in complex situations where risks may be poorly formalized and difficult to quantify.

Therefore, it is recommended to use a combination of both approaches to obtain more complete and refined risk information. This will allow for the development of more informed cybersecurity risk management strategies and ensure the efficient allocation of funds for the implementation of preventive security measures and the protection of important critical infrastructure.

A combined approach to cyber threat risk assessment that combines approaches based on averages and fuzzy set theory can have several advantages.

More comprehensive risk assessment. The combination of the two approaches allows you to take into account both average values and data that are unclear or ambiguous. This provides a more complete risk assessment, as it takes into account both the main trends and possible variations and uncertainties.

More adaptive solutions. Combining approaches allows taking into account different aspects of risk. On the one hand, taking into account average values can help to understand the overall picture, and on the other hand, fuzzy set theory can provide more flexible and adaptive assessments in conditions of instability or ambiguity.

Improved decision-making. Combining different approaches can help to avoid distortions or biases that can result from using only one method. This can improve the accuracy of the assessment and make decision-making more informed.

References

[1] Bek U. Obshhestvo riska. Na puti k drugomu modernu. Per. s nem. V. Sedel'niku i N.Fèdorovoj. Moskva: Progress-Tradicija, 2000. 384 s.

[2] Oleksandr Korystin, Nataliia Svyrydiuk. “Activities of Illegal Weapons Criminal Component of Hybrid Threats”. Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021). Series: Advances in Social Science, Education and Humanities Research, vol. 170, 22 March 2021, pp. 86-91.

[3] Nazareth, Derek L., and Jae Choi (2015). A system dynamics model for information security management, Information & Management. Vol. 52 (1). Pp. 123-134.

[4] Joshi, Chanchala, and Umesh Kumar Singh (2017). “Information security risks management framework–A step towards mitigating security risks in university network”. Journal of Information Security and Applications. Vol. 35. Pp. 128-137.

[5] Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed (2016). Information securi ty management needs more holistic approach: A literature review. International Journal of Information Management. Vol. 36 (2). Pp. 215-225.

[6] Nitin Deepak, Shishir Kumar, "Flexible Self-Managing Pipe-line Framework Reducing Development Risk to Improve Software Quality", International Journal of Information Technology and Computer Science, vol.7, no.7, pp.35-47, 2015.

[7] Adil Bashir, Sahil Sholla, "Resource Efficient Security Mechanism for Cloud of Things", International Journal of Wireless and Microwave Technologies, Vol.11, No.4, pp. 41-45, 2021.

[8] Shuaiqi Zhang, "Some Results on Optimal Dividend Problem in Two Risk Models", International Journal of Information Engineering and Electronic Business, Vol. 2, No.2, pp.24-30, 2010.

[9] Peltier, Thomas R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications.

[10] Layton, Timothy P. (2016). Information Security: Design, implementation, measurement, and compliance. Auerbach Publications.

[11] Yoon, Junseob, and Kyungho Lee (2016). Advanced assessment model for improving effective ness of information security measurement. International Journal of Advanced Media and Communication. Vol. 6 (1). Pp. 4-19.

[12] Hakan Kekül, Burhan Ergen, Halil Arslan (2022). Estimating Missing Security Vectors in NVD Database Security Reports. International Journal of Engineering and Manufacturing, Vol. 12. No. 3. Pp. 1-13.

[13] P. Mell, K. Scarfone, and S. Romanosky (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. FIRSTForum of Incident Response and Security Teams.

[14] G. Spanos, A. Sioziou, and L. Angelis (2013). WIVSS: A New Methodology for Scoring Information Systems Vulnerabilities, Proceedings of the 17th Panhellenic Conference on Informatics. Pp. 83–90.

[15] Hakan Kekül, Burhan Ergen, Halil Arslan (2021). A New Vulnerability Reporting Framework for Software Vulnerability Databases, International Journal of Education and Management Engineering. Vol. 11. No. 3. Pp. 11-19.

[16] M. M. A. Muhammad Noman Khalid, Muhammad iqbal, Kamran Rasheed (2020). Web Vulnerability Finder (WVF): Automated Black- Box Web Vulnerability Scanner, International Journal of Information Technology and Computer Science, Vol. 12. No. 4. Pp. 38–46.

[17] Abhinandan H. Patil, Neena Goveas, Krishnan Rangarajan,"Regression Test Suite Prioritization using Residual Test Coverage Algorithm and Statistical Techniques", International Journal of Education and Management Engineering, Vol.6, No.5, pp.32-39, 2016.

[18] R. Ranjan, G. Sahoo (2014). A new clustering approach for anomaly intrusion detection. International Journal of Data Mining & Knowledge Management Process (IJDKP). Vol. 4. No. 2. Pp. 29–38.

[19] Serhii Zybin, Yana Bielozorova, "Risk-based Decision-making System for Information Processing Systems", International Journal of Information Technology and Computer Science, Vol.13, No.5, pp.1-18, 2021.

[20] I. Parkhomey, S. Gnatyuk, R. Odarchenko, T. Zhmurko et al, “Method for UAV Trajectory Parameters Estimation Using Additional Radar Data”, Proceedings of the 2016 4th International Conference on Methods and Systems of Navigation and Motion Control, Kyiv, Ukraine, October 18-20, 2016, pp.39-42.
[21] F. Adeyinka, E. S. Oluyemi, A. N. Victor, U. C. Uchenna, O. Ogedengbe, S. Ale (2017). Parametric Equation for Capturing Dynamics of Cyber Attack Malware Transmission with Mitigation on Computer Network, International Journal of Mathematical Sciences and Computing, Vol. 3. No. 4. Pp. 37-51.
[22] Y. Ghaderipour, H. Dinari (2020). A Flow-Based Technique to Detect Network Intrusions Using Support Vector Regression (SVR) over Some Distinguished Graph Features, International Journal of Mathematical Sciences and Computing. Vol. 6. No. 4. Pp.1-11.
[23] Pyskun Igor, Tkach Yuliia, Khoroshko Volodymyr, Khokhlachova Yulia, Ayasrah Ahmad Rasmi Ali, Al-Dalvash Ablullah Fowad, Quantitative assessment and determination of the level of cyber security of state information systems, Ukrainian Scientific Journal of Information Security, Vol. 26 No. 3, Pp. 31-138, 2020.
[24] Korchenko Anna, Shcherbina Vladimir, Vishnevskaya Natalia A methodology for building cyberattack-generated anomaly detection systems, Ukrainian Information Security Research Journal, Vol. 18 No.1, Pp.312-324, 2016.
[25] Nikolay Karpinsky, Anna Korchenko, Sanzira Akhmetova The method of development of basic detection rules for intrusion detection systems, Ukrainian Information Security Research Journal, Vol.17, No.4, Pp.30-38, 2015.
[26] Oleksandr Korystin, Svyrydiuk Nataliia, Olena Mitina, "Risk Forecasting of Data Confidentiality Breach Using Linear Regression Algorithm", International Journal of Computer Network and Information Security, Vol.14, No.4, pp.1-13, 2022.
[27] Serhii Zybin, Yana Bielozorova, "Risk-based Decision-making System for Information Processing Systems", International Journal of Information Technology and Computer Science, Vol.13, No.5, pp.1-18, 2021.
[28] Gulzhanat Beketova, Berik Akhmetov, Alexander Korchenko, Valery Lakhno Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features, Ukrainian Scientific Journal of Information Security, Vol. 22, No.3, Pp.242-254, 2016.
[29] O.G. Korchenko, S.V. Kazmirchuk, B.B. Akhmetov, Applied information security risk assessment systems. Monograph, Kyiv, CP "Comprint", 435 p., 2017.
[30] L. -Y. Chang and Z. -J. Lee, "Applying fuzzy expert system to information security risk Assessment - A case study on an attendance system", 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), Taipei, Taiwan, 2013, pp. 346-351.
[31] S. A. Abdymanapov, M. Muratbekov, S. Altynbek and A. Barlybayev, "Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems," in IEEE Access, vol. 9, pp. 156556-156565, 2021.
[32] F. Z. Gozon, D. Vaczi and E. Toth-Laufer, "Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment," 2021 IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 2021, pp. 83-88.
[33] K. S. Duisebekova and T. Duisebekov, "Utilization of Fuzzy Mathematics for Security Model of a System," 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), Almaty, Kazakhstan, 2018, pp.1-6.
[34] W. Shang, T. Gong, J. Hou, J. Lu and Z. Cao, "Quantitative Evaluation Method for Industrial Control System Vulnerability Based on Improved Expert Elicitation and Fuzzy Set Method", in IEEE Access, vol. 11, pp. 101007-101019, 2023.
[35] Higgins, J. et al., 2019. Cochrane Handbook for Systematic Reviews of Interventions, 2nd Edition ed. Chichester (UK): John Wiley & Sons.
[36] Weidt, F. & Silva, R., 2016. Systematic Literature Review in Computer Science-A Practical Guide, Relatórios Técnicos do DCC/UFJF, 1(0), pp.1-7.
[37] Ralph Eckmaier, Walter Fumy, Stéfane Mouille, Jean-Pierre Quemard, Nineta Polemi, Rainer Rumpel. (2022) Risk Management Standards. Analysis of standardisation requirements in support of cybersecurity policy. ENISA.
[38] Stouffer, K. et al., 2015. Guide to Industrial Control Systems (ICS) Security.
[39] Alberts, C., Behrens, S., Pethia, R. & Wilson, W., 1999. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.
[40] Costas Lambrinoudakis, Stefanos Gritzalis, Christos Xenakis, Sokratis Katsikas, Maria Karyda, Aggeliki Tsochou European Union Agency for Cybersecurity (2022). Compendium of Risk Management Frameworks with Potential Interoperability.
[41] Korystin, O.Ye. & Korystin, O.O. (2022), “Threats in the sphere of cyber security in Ukraine”, Nauka i pravookhoronna, vol. 1, pp. 127–131.
[42] Goldammer, P., Annen, H., Stöckli, P. L., & Jonas, K. (2020). Careless responding in questionnaire measures: Detection, impact, and remedies. The Leadership Quarterly, 31(4), 101384.
[43] Oleksandr Korystin, Nataliia Svyrydiuk, Alexander Vinogradov. “The Use of Sociological Methods in Criminological Research”, Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021). Series: Advances in Social Science, Education and Humanities Research, vol. 617, 18 December 2021, pp.1-6.
[44] ISO 31000:2018 - Risk Management, URL: https://www.iso.org/ru/publication/PUB100464.html
[45] Korystin O., Svyrydiuk N. Methodological principles of risk assessment in law enforcement activity. Nauka i pravooxoronna. No. 3, P.191-197, 2020.
[46] Oleksandr Korystin, Nataliia Svyrydiuk, Volodymyr Tkachenko, “Fiscal Security of the State Considering Threats of Macroeconomic Nature”. Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL2021). Series: Advances in Social Science, Education and Humanities Research, vol. 188, 27 August 2021, pp. 65-691.
[47] Morklyanik B., Korchenko O., Kubiv S., Kazmirchuk S., Teliushchenko V. The method of phasification of intervals for solving cybersecurity assessment tasks at critical infrastructure facilities, Ukrainian Scientific Journal of Information Security, Tom. 29, Vol.3, Pp.103-113, 2023.
[48] A. Korchenko, V. Breslavskyi, S. Yevseiev, N. Zhumangalieva, A. Zvarych, S. Kazmirchuk, O. Kurchenko, O. Laptiev, O. Sievierinov, S. Tkachuk, Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency, Eastern-European Journal of Enterprise Technologies, Vol.111. No.3/9, Pp. 63-83, 2021.

Authors' Profiles

Oleksandr Evgeniyovych Korystin

DSc (Law), Professor. In 2009 he received DSc degree in information law from NAIA. In 2014 he received Professor degree. Honored Academic of Science and Technology of Ukraine.

Chief Research Scientist of the Criminological Research Laboratory of the State Scientific Research Institute of the Ministry of Internal Affairs of Ukraine. Professor of the National Academy of the Security Service of Ukraine. In 2014–2016 – Rector of the Odesa State University of Internal Affairs. Head of the Risk Management & Resilience Committee NGO "Institute of Cyber Warfare Research". Research interests: cybersecurity; criminology; economic security; intelligence; methodology of strategical (SWOT-analysis; risks assessment); cyber resilience, counteraction to the hybrid threat.

Oleksandr Korchenko

Dr. habil. (cybersecurity), Professor. In 2004, he defended his thesis and received the diploma of Doctor of Technical Sciences. In 2005, he was awarded the title of professor of the IT-Security Academic Department National Aviation University. Honored Academic of Science and Technology of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology. Recognized as a qualified doctor and titular professor in Poland.

Vice-Rector for Research of the National Aviation University. In 2004–2023 – Head (Chairman) of IT-Security Academic Department of the National Aviation University. Head of Information Systems &Technologies Security Academic Department of the National Education Commission of the University, Krakow, Poland. There is a Senior Member IEEE.

Research interests: information security, fuzzy logic, risk assessment, information security incident management, cybersecurity, intellectual information security systems.

Svitlana Kazmirchuk

DSc Eng, Professor. In 2018, she defended his thesis and received the diploma of Doctor of Technical Sciences. In 2021, she was awarded the title of professor of the IT-Security Academic Department, National Aviation University.

Professor of the IT-Security Academic Department National Aviation University. In 2018–2023 – Head (Chairman) of Academic Department Computerized information security systems (National Aviation University). Research interests: information security, fuzzy logic, risk assessment, information security incident management, cybersecurity, information security management system.

Serhii Demediuk

Ph.D (Law), Deputy Secretary of the National Security and Defense Council of Ukraine. Deputy Head of the National Coordination Center for Cyber Security. Professor of the Cybersecurity Department of the National Academy of the Security Service of Ukraine. From 2015 to 2019 - Chief of the Cyber Police of Ukraine.

Research interests: information security, cybersecurity, cyber warfare, cybercrime, cyber resilience, intelligence, counteraction to the hybrid threat.

Oleksandr Oleksandrovych Korystin

In 2021, he received a bachelor's degree in cyber security at the National Aviation University. Master's student of NAU, majoring in cyber security. Receives a bachelor's degree in computer Engineering National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (FICT, 4th year).

Research interests: information security, cybersecurity, cybercrime, risk assessment.

How to cite this paper: Oleksandr Evgeniyovych Korystin, Oleksandr Korchenko, Svitlana Kazmirchuk, Serhii Demediuk, Oleksandr Oleksandrovych Korystin, "Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.1, pp.24-34, 2024. DOI:10.5815/ijcnis.2024.01.02