IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 1, February, 2023, pp. 77-84
Journal homepage: http://iieta.org/journals/isi

Ranking Threats to Determine the Cost of Protecting Information in a Cybersecurity Environment

Vladislav Yemanov[1*], Vasyl Pasichnyk[2], Ihor Yevtushenko[3], Stanislav Larin[4], Olena Mykhailenko[5]

[1] National Academy of the National Guard of Ukraine, Kharkiv 39000, Ukraine
[2] Department of State Policy and Governance, Lviv Polytechnic National University, Lviv 79000, Ukraine
[3] Institute for the Security Service of Ukraine, Yaroslav Mudryi National Law University, Kharkiv 39000, Ukraine
[4] State Institution of Higher Education, University of Educational Management of National Academy of Educational Sciences of Ukraine, Kyiv 59000, Ukraine
[5] Department of Technical Mechanics, Tavriy State Agrotechnological University named after Dmytro Motorny, Melitopol 19000, Ukraine

Corresponding Author Email: pasichnyk.vasyl.edu@gmail.com

https://doi.org/10.18280/isi.280108

Received: 17 December 2022
Accepted: 12 February 2023

Keywords:
information, cybersecurity, threats, security, ranking

ABSTRACT

The main purpose of the study is to rank certain threats in order to establish further costs for ensuring the protecting of information in the cybersecurity system. Research methodology is a set of methods that form a methodological approach. The main ones are the ranking method through the theory of fuzzy relations and the expert-step method. As a result, due to the ranking of the threats of the selected object, the permissible intensity of the decrease in the level of security and the costs of its provision were determined using the proposed methodology. The results obtained implied the use of modern ranking methods according to the given parameters. In our case, the results obtained allowed us to rank the existing list of threats in the cybersecurity system. The benefit of such results lies in the formation of an information basis for the adoption and implementation of management decisions.The study is limited by selecting only one socio-economic system and its information. The results obtained out in the article have practical and scientific value through a methodical approach to form requirements for the security of the cybersecurity system itself and information of a single object. In the future, more complex socio-economic systems and their cybersecurity should be chosen to apply the methodological approach proposed in the article.

1. INTRODUCTION

Important methods for analyzing the state of ensuring cybersecurity are methods of description and classification. To implement effective information protection, one should firstly describe and then classify various types of threats and dangers, risks and challenges and, accordingly, formulate a system of measures to manage them. As common methods for analyzing the level of ensuring cybersecurity, methods of studying causal relationships are used. Using these methods, causal relationships between threats and hazards are revealed; a search is made for the causes that have become the source and led to the actualization of certain hazard factors, and measures are being developed to neutralize them. The choice of methods for analyzing the state of ensuring cybersecurity depends on the specific level and scope of protection organization. Depending on the threat, it is possible to differentiate both different levels of threats and different levels of protection.

An important factor in the development of modern society is to ensure the protection of information and cybersecurity, which is a key element of any processes, regardless of the scope of public activity. At the same time, special attention is paid to the analysis of potential threats, the implementation of which leads to material, financial, reputational and other losses.

To counter cybersecurity threats, the necessary measures are taken both in the direction of exerting a certain influence on the source of the threat, and in the direction of reducing the vulnerabilities of the security object. Accordingly, two subject areas of counteraction are distinguished: one of them is formed by a combination of threat sources, and the other by a combination of measures to ensure cybersecurity. Therefore, we can conclude that information and cybersecurity cover technical, legal, organizational, psychological aspects and causes the extreme complexity and multi-level system links between its constituent elements. In turn, ensuring cybersecurity is a continuous process that is systemic in nature and is achieved by implementing the most rational methods and comprehensively using the necessary means (physical, hardware, software, cryptographic). Moreover, the best result is obtained when all the means and methods used are combined into an integral mechanism, the functioning of which must be monitored, updated and supplemented depending on changes in both the internal and external environment. In addition, it should be noted that this process must be accompanied by proper training of industry specialists, administration, employees, users and their compliance with all established rules.

The main purpose of the study is to rank certain threats in order to establish further costs for ensuring the protecting of information in the cybersecurity system. To do this, we need

to properly structure our study. The existing literature should be reviewed for research. In detail, present the methods used. Present the results of the study. Compare the results of the study with existing ones on similar topics. Describe the findings and further scientific plans on this topic.

2. LITERATURE REVIEW

In general, according to our research agenda, scientists agree in the scientific literature that the modern information space is affected by a wide variety of threats, the implementation of which can lead to extremely negative consequences. Therefore, the study of the impact of threats on the level of security of systems is an urgent and important scientific task, characterized by a high degree of uncertainty and the complexity of rigorous formalization [1-3].

The rapid development of information technologies and their introduction into all spheres of public life determines the extreme importance of creating reliable information protection systems. The problem of the qualitative functioning of these systems, given the emergence of new and the growth of the level of existing threats in the information space, is becoming increasingly important. Moreover, an important practical problem is to establish the optimal balance between ensuring the security of the security system and the amount of costs for its support, given the rational distribution between individual areas of protection. In the vast majority of cases, this issue is solved with the help of statistical analysis methods that require consideration of a significant amount of information, complex calculations, and take a long time to process [4-6].

As most scientists note [7-9], in today's globalized world, information and databases are those unique resources without the use and preservation of which it is impossible to exist and develop both a modern state, as a socio-political entity, and the fulfillment of purely military tasks to preserve independence. and defense of the country. According to expert circles and analysts from the leading countries of the world, the hybrid nature of a modern armed conflict is determined precisely by the presence of a powerful information and cybernetic component. Access to information and protection of management processes are becoming the determining factors in achieving political goals and the troops of a new victory.

Most scientists [10-12] describe in the scientific literature, the practice that new destructive practices are developing in cyberspace, including the criminal use of the Internet (cybercrime), espionage for political or economic purposes, as well as attacks on critical infrastructure (transport, transport communications and etc.) for sabotage purposes. Coming from their governments or non-government players, these cyber attacks are: not limited by borders or distance; are anonymous and it is very difficult to really identify the real culprit, often operating under the guise of botnets or intermediaries; can be done with relative ease, at little cost or risk to the attacker. They aim to jeopardize the smooth functioning of information and communication systems used by citizens, businesses and administrations, as well as the physical integrity of infrastructure, which is critical to national security.

Since we are in our threat ranking study, the literature on this topic should be reviewed. In general, scientists agree [11-13] that threats characterize the possible actions that can be taken against the system and can lead to a violation of basic services, for example: integrity, confidentiality, availability, reliability of information. They appear in different forms.

There are many cybersecurity threats that, according to certain characteristics, belong to one class or another. To prevent, eliminate or reduce the impact of these threats, it is necessary to analyze them and create a threat model. That is why the problem of ranking cybersecurity threats for a particular socio-economic system and its information support is relevant and kind of new.

3. METHODOLOGY

In the beginning, it should be noted that any important scientific research should include a number of well-known theoretical methods, without which it is impossible to effectively investigate the problem. We also used theoretical methods of analysis, synthesis, abstract-logical, etc. All of them allowed a better understanding of the subject of research, but their detailed description is not necessarily here.

The main research method is the ranking method using the theory of fuzzy relations. The best description of a given method is through its practical application. Therefore, the work of the method will be presented below in the text of the article.

For our study, a real-life socio-economic system with its own cybersecurity system and information security elements is needed for a good example of the research results. The proposed research methodology will be difficult to present only in a theoretical form, which is why it should be applied in practice. It should be noted that the choice of Sigma Software is presented purely from subjective views, since it has all the elements necessary for analysis and meets all the parameters. The choice of other socio-economic systems is possible in further research.

Of course, in addition to the methods presented above, an expert method was applied with the involvement of experts from «Sigma Software» and specialists in information security and cybersecurity. All agreed experts were selected according to the criteria, however, their evaluation is purely subjective in order to help demonstrate the effectiveness of the methodology and our study as a whole.

With the assistance of the expert method, we can identify the most important from the subjective point of view of experts and our threat to information security in the Sigma Software cybersecurity system: natural phenomena and man-made negative impact (K_1); military invasion (K_2); terrorist impact (K_3); industrial espionage (K_4); hacker influence (K_5); insider influence (K_6); security of communication channels of the socio-economic system (K_7); unreliability of the security components of service systems (K_8); insecurity of databases and cloud services (K_9); danger of Internet resources (K_{10}); malware (K_{11}); DoS attacks (K_{12}).

But, the question arises what exactly these threats affect in the context of the cybersecurity and information protection system. Thus, the aforementioned threats are expressed in violation of the following Sigma Software information security criteria: information availability (C_1), information integrity (C_2), information confidentiality (C_3), information reliability (C_4). In total, they form a set of criteria, which we denote mathematically as C_j.

It is μ_{ij} that is a value within the corridor interval from 0 to 1 and will characterize the level of impact of information security threats (K_i) determined by the expert method on failure to fulfill one of the criteria that were also presented

above in the text of the methodology (C_j). That is, μ_{ij} is a number from the interval [0, 1], which characterizes the degree of influence of K_i threats on non-fulfillment of the C_j criterion. The following equality (1) must be satisfied:

$$I_i=\{\mu_{i1}/C_1, \mu_{i2}/C_{2,\ldots..}, \mu_{im}/C_m\} \quad (1)$$

The determination of μ_{ij} will be carried out using the method of least impact, the description of which does not require detailing, which is well known in econometric scientific directions.

4. RESULTS OF RESEARCH

Thus, we will rank information security threats in the cybersecurity system («Sigma Software» based on the methods described above. To begin with, we will present the initial data for the least impact method according to expert comparisons of the impact powers f_{ij} with the lowest impact forces f_{il} (Table 1).

Table 1. Initial data for the calculations made

K_i	C_1	f_{ij}/f_{il}			
		C_1	C_2	C_3	C_4
K_1	C_3	11/13=8	12/13=5	13/13=1	14/13=1
K_2	C_4	21/24=7	22/24=4	23/24=5	24/24=1
K_3	C_4	31/34=6	32/34=9	33/34=2	34/34=1
K_4	C_1	41/41=1	42/41=3	43/41=9	44/41=5
K_5	C_4	51/54=5	52/54=7	53/54=6	54/54=1
K_6	C_1	61/61=1	62/61=5	63/61=7	64/61=4
K_7	C_2	71/72=8	72/72=1	73/72=5	74/72=3
K_8	C_3	81/83=9	82/83=6	83/83=1	84/83=4
K_9	C_1	91/91=1	92/91=4	93/91=3	94/91=1
K_{10}	C_4	101/104=4	102/104=1	103/104=5	104/104=1
K_{11}	C_4	111/114=5	112/114=8	113/114=6	114/111=1
K_{12}	C_3	121/123=9	122/123=1	123/123=1	124/123=1

By itself, C_j can contain all admissible and possible criteria, which, in turn, the threats to the security of information defined by us in the cybersecurity system K_i have one of the least influences. Then f_{ij}/f_{il} represent a comparison of the impact powers f_{ij} with the lowest impact levels f_{il}..

The next step is to calculate the least possible degree of influence of certain threats (K_i) for the information protection system in cybersecurity «Sigma Software» (2):

$$\mu_{i1}=\{f_{i1}/f_{ij}, f_{i2}/f_{ij,\ldots..}, f_{im}/f_{ij}\}^{-1} \quad (2)$$

Based on this (2) it is easy to calculate the desired degree of impact, which will correspond to each of the pairs (K_i ,C_j) (3):

$$\mu_{i1}=\mu_{il}(f_{i1}/f_{ij}),\ \mu_{i2}=\mu_{il}(f_{i2}/f_{ij}),\ \ldots..,\ \mu_{im}=\mu_{il}(f_{im}/f_{ij}), \quad (3)$$

Based on the data from Table 1, we can determine the degrees of influence μ_{ij}, and they in turn form a fuzzy relation as such (Table 2). For all tables, there is a certain standardization laid down by the chosen methodological approach, however, an individual approach is inherent in certain tables, according to the course of the study.

Thus, Table 2 should be normalized by dividing its elements in each row by the maximum of the allowed values and we will get Table 3.

Table 2. Determination of the degree of impact

I			
8/15	5/15	1/15	1/15
7/17	4/17	5/17	1/17
6/18	9/18	2/18	1/18
1/18	3/18	9/18	5/18
5/19	7/19	6/19	1/19
1/17	5/17	7/17	4/17
8/17	1/17	5/17	3/17
9/20	6/20	1/20	4/20
1/9	4/9	3/9	1/9
4/11	1/11	5/11	1/11

Table 3. The ratio normalization

I			
1.0	0.63	0.13	0.13
1.0	0.57	0.71	0.14
0.67	1.0	0.22	0.11
0,11	0.33	1.0	0.56
0.71	1.0	0.86	0.14
0.14	0.71	1.0	0.57
1.0	0.13	0.63	0.38
1.0	0.67	0.11	0.44
0.25	1.0	0.75	0.25
0.8	0.2	1.0	0.2

The next step involves the definition of a fuzzy similarity relation, which should be formed from the set of values of the very degree of similarity (r_{ij}) (4):

$$R=[r_{ij}/(K_i,K_j] \quad (4)$$

It should be noted that $r_{ij}=1-d_{ij}$ should hold, where d_{ij} is a kind of distance between the fuzzy set of threat impacts K_i and K_j (5):

$$\begin{aligned} I_i&=\{\mu_{i1}/K_1, \mu_{i2}/K_{2,\ldots..}, \mu_{im}/K_m\} \\ I_j&=\{\mu_{j1}/K_1, \mu_{j2}/K_{2,\ldots..}, \mu_{jm}/K_m\} \end{aligned} \quad (5)$$

Next, use the relative Euclid ($d_{ij}^{(e)}$) and Hamming ($d_{ij}^{(h)}$) to calculate d_{ij} (6):

$$\begin{aligned} d_{ij}^{(h)}&=1/n\sum[\mu_{ik}-\mu_{jk}] \\ d_{ij}^{(e)}&=1/n\sqrt{\sum(\mu_{ik}-\mu_{jk})^2} \end{aligned} \quad (6)$$

Let's present the completed matrix of the fuzzy similarity relation with the corresponding properties of reflectivity and symmetry inherent in the research methodology (Table 4).

One of our tasks is to divide the selected set of threats into classes that, under no circumstances, do not intersect, but, in addition, must contain elements that are similar in degree of impact. To do this, let's give the original similarity relation R the so-called transitivity property. The calculation takes place through the maximum product of the corresponding matrices through the corresponding calculations. In order to divide the set of threats into non-overlapping classes and containing elements similar in degree of impact, it is necessary to give the initial non-transitive similarity relation R the property of transitivity. Such a transformation is provided by the operation of transitive closure of a fuzzy relation. As a result, we get Table 5 for R^2, R^3, R^4.

Let's do the same for R^5, R^6 (Table 6).

Table 4. Filled matrix of fuzzy relation of similarity

R											
1	0.84	0.81	0.38	0.65	0.44	0.69	0.91	0.53	0.61	0.59	0.86
0.84	1	0.68	0.54	0.76	0.57	0.81	0.75	0.67	0.76	0.76	0.73
0.81	0.68	1	0.38	0.82	0.48	0.53	0.72	0.73	0.55	0.85	0.67
0.38	0.54	0.38	1	0.54	0.88	0.59	0.44	0.66	0.7	0.53	0.39
0.65	0.76	0.82	0.54	1	0.64	0.59	0.58	0.83	0.73	0.95	0.51
0.44	0.57	0.48	0.88	0.64	1	0.5	0.52	0.76	0.61	0.63	0.3
0.69	0.81	0.53	0.59	0.59	0.5	1	0.72	0.53	0.76	0.6	0.8
0.91	0.75	0.72	0.44	0.58	0.52	0.72	1	0.52	0.55	0.59	0.78
0.53	0.67	0.73	0.66	0.83	0.76	0.53	0.52	1	0.59	0.87	0.39
0.61	0.76	0.55	0.7	0.73	0.61	0.76	0.55	0.59	1	0.68	0.68
0.59	0.76	0.85	0.53	0.95	0.63	0.6	0.59	0.87	0.68	1	0.52
0.86	0.73	0.67	0.39	0.51	0.3	0.8	0.78	0.39	0.68	0.52	1

Table 5. The results of the calculations for R^2, R^3, R^4

R^2											
1	0.84	0.81	0.61	0.81	0.64	0.81	0.91	0.73	0.76	0.81	0.86
0.84	1	0.81	0.7	0.76	0.67	0.76	0.84	0.76	0.76	0.76	0.84
0.81	0.81	1	0.66	0.85	0.73	0.85	0.81	0.85	0.73	0.85	0.81
0.61	0.7	0.66	1	0.7	0.88	0.7	0.59	0.76	0.7	0.68	0.68
0.81	0.76	0.85	0.7	1	0.76	1	0.75	0.87	0.76	0.95	0.73
0.64	0.67	0.73	0.88	0.76	1	0.61	0.59	0.76	0.7	0.76	0.61
0.81	0.81	0.72	0.7	0.76	0.61	0.59	0.78	0.67	0.76	0.76	0.8
0.91	0.84	0.81	0.59	0.75	0.59	0.76	1	0.72	0.75	0.75	0.86
0.73	0.76	0.85	0.76	0.87	0.76	0.67	0.72	1	0.73	0.87	0.67
0.76	0.76	0.73	0.7	0.76	0.7	0.76	0.75	0.73	1	0.76	0.76
0.81	0.76	0.85	0.68	0.95	0.76	0.76	0.75	0.87	0.76	1	0.73
0.86	0.84	0.81	0.68	0.73	0.61	0.8	0.86	0.67	0.76	0.73	1
R^3											
1.0	0.84	0.81	0.7	0.81	0.73	0.81	0.91	0.81	0.76	0.81	0.86
0.84	1.0	0.81	0.7	0.81	0.76	0.81	0.84	0.76	0.76	0.81	0.84
0.81	0.81	1.0	0.73	0.85	0.76	0.81	0.81	0.85	0.76	0.85	0.81
0.7	0.7	0.73	1.0	0.76	0.88	0,7	0.7	0.76	0.7	0.76	0,7
0.81	0.81	0.85	0.76	1.0	0.76	0.76	0.81	0.87	0.76	0.95	0.81
0.73	0.76	0.76	0.88	0.76	1.0	0.7	0.72	0.76	0.73	0.76	0.68
0.81	0.81	0.81	0.7	0.76	0.7	1.0	0.81	0.76	0.76	0.76	0.81
0.91	0.84	0.81	0.7	0.81	0.72	0.81	1.0	0,75	0.76	0.81	0.86
0.81	0.76	0.85	0.76	0.87	0.76	0.76	0,75	1.0	0.76	0.87	0.73
0.76	0.76	0.76	0.7	0.76	0.73	0.76	0.76	0.76	1.0	0.76	0.76
0.81	0.81	0.85	0.76	0.95	0.76	0.76	0.81	0.87	0.76	1.0	0.81
0.86	0.84	0.81	0.7	0.81	0.68	0.81	0.86	0.73	0.76	0.81	1.0
R^4											
1.0	0.84	0.81	0.73	0.81	0.76	0.81	0.91	0.81	0.76	0.81	0.86
0.84	1.0	0.81	0.76	0.81	0.76	0.81	0.84	0.81	0.76	0.81	0.84
0.81	0.81	1.0	0.76	0.85	0.76	0.81	0.81	0.85	0.76	0.85	0.81
0.73	0.76	0.76	1.0	0.76	0.88	0.7	0.72	0.76	0.73	0.76	0,7
0.81	0.81	0.85	0.76	1.0	0.76	0.81	0.81	0.87	0.76	0.95	0.81
0.76	0.76	0.76	0.88	0.76	1.0	0.76	0,75	0.76	0.76	0.76	0.73
0.81	0.81	0.81	0,7	0.81	0.76	1.0	0.81	0.76	0.76	0.81	0.81
0.91	0.84	0.81	0.72	0.81	0,75	0.81	1.0	0.81	0.76	0.81	0.86
0.81	0.81	0.85	0.76	0.87	0.76	0.76	0.81	1.0	0.76	0.87	0.81
0.76	0.76	0.76	0.73	0.76	0.76	0.76	0.76	0.76	1.0	0.76	0.76
0.81	0.81	0.85	0.76	0.95	0.76	0.81	0.81	0.87	0.76	1.0	0.81
0.86	0.84	0.81	0.7	0.81	0.73	0.81	0.86	0.81	0.76	0.81	1.0

Table 6. The results of the calculations for R^5, R^6

R^5											
1.0	0.84	0.81	0.76	0.81	0.76	0.81	0.91	0.81	0.76	0.81	0.86
0.84	1.0	0.81	0.76	0.81	0.76	0.81	0.84	0.81	0.76	0.81	0.84
0.1	0.81	1.0	0.76	0.85	0.76	0.81	0.81	0.85	0.76	0.85	0.81
0.76	0.76	0.76	1.0	0.76	0.88	0.76	0.75	0.76	0.76	0.76	0.73
0.81	0.81	0.85	0.76	1.0	0.76	0.81	0.81	0.87	0.76	0.95	0.81
0.76	0.76	0.76	0.88	0.76	1.0	0.76	0.76	0.76	0.76	0.76	0.76
0.81	0.81	0.81	0.76	0.81	0.76	1.0	0.81	0.81	0.76	0.81	0.81
0.91	0.84	0.81	0.75	0.81	0.76	0.81	1.0	0.81	0.76	0.81	0.86
0.81	0.81	0.85	0.76	0.87	0.76	0.81	0.81	1.0	0.76	0.87	0.81
0.76	0.76	0.76	0.76	0.76	0.76	0.76	0.76	0.76	1.0	0.76	0.76

0.81	0.81	0.85	0.76	0.95	0.76	0.81	0.81	0.87	0.76	1.0	0.81
0.86	0.84	0.81	0.73	0.81	0.76	0.81	0.86	0.81	0.76	0.81	1.0

R^6

1.0	0.84	0.81	0.76	0.81	0.76	0.81	0.91	0.81	0.76	0.81	0.86
0.84	1.0	0.81	0.76	0.81	0.76	0.81	0.84	0.81	0.76	0.81	0.84
0.81	0.81	1.0	0.76	0.85	0.76	0.81	0.81	0.85	0.76	0.85	0.81
0.76	0.76	0.76	1.0	0.76	0.88	0.76	0.76	0.76	0.76	0.76	0.76
0.81	0.81	0.85	0.76	1.0	0.76	0.81	0.81	0.87	0.76	0.95	0.81
0.76	0.76	0.76	0.88	0.76	1.0	0.76	0.76	0.76	0.76	0.76	0.76
0.81	0.81	0.81	0.76	0.81	0.76	1.0	0.81	0.81	0.76	0.81	0.81
0.91	0.84	0.81	0.76	0.81	0.76	0.81	1.0	0.81	0.76	0.81	0.86
0.81	0.81	0.85	0.76	0.87	0.76	0.81	0.81	1.0	0.76	0.87	0.81
0.76	0.76	0.76	0.76	0.76	0.76	0.76	0.76	0.76	1.0	0.76	0.76
0.81	0.81	0.85	0.76	0.95	0.76	0.81	0.81	0.87	0.76	1.0	0.81
0.86	0.84	0.81	0.76	0.81	0.76	0.81	0.86	0.81	0.76	0.81	1.0

Our calculations led to the fact that $R^3 = R^4 ..... = R^n$. Thus, the ratio R will be in the following form (7):

$$R=R\cup R^2\cup R^3\cup ....\cup R^k \cup ....=R^6 \quad (7)$$

Next, the ranks of threats to information security in the cybersecurity system should be determined ($\rho_i = \sum_{i=1}^{m} \mu_{ij}$). Everything is simple. The value of the rows from Table 3 should be summed up, and we will find the ranks of the threats: $\rho_1=1.89$; $\rho_2=\rho_6=2.42$; $\rho_3=\rho_4=2$; $\rho_5=2.71$; $\rho_7=2.14$; $\rho_8=2.22$; $\rho_9=2.25$; $\rho_{10}=2.2$; $\rho_{11}=2.51$; $\rho_{12}=1.33$.

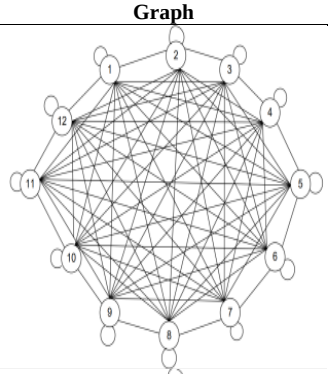
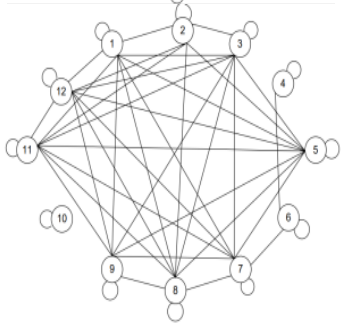
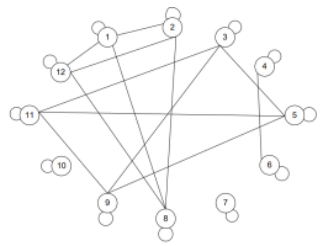
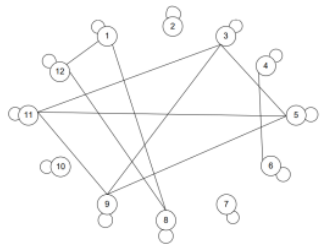
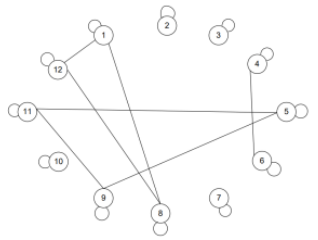
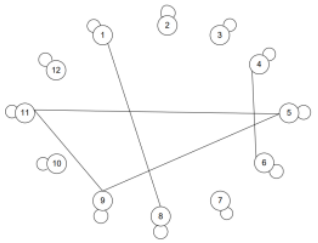
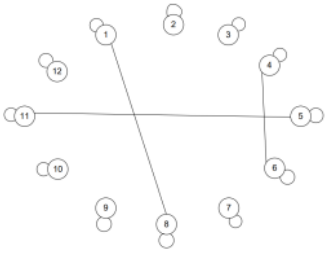
By itself, we arrange the fuzzy relation R according to α - levels and get (8):

$$R=\cup\alpha R_\alpha=0.76R_{0.76}\cup 0.81R_{0.81}\cup 0.84R_{0.84}\cup 0.85R_{0.85}\cup 0.86R_{0.86}\cup 0.87R_{0.87}\cup 0.88R_{0.88}\cup 0.91R_{0.91}\cup 0.95R_{0.95}\cup R_1 \quad (8)$$

Level α relations with graphs are presented in Table 7.

As a result, we have the fact that the ratio α-level forms the classes of information protection threats in the cyber security system that are equivalent in importance to us (Table 8).

Table 7. Level α relations with graphs

α	R_α	Graph
0.76	1 1	
0.81	1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 0 1 1	
0.84	1 1 0 0 0 0 0 1 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0	
0.85	0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0	
0.86	0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0	
0.87	0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0	
0.88	0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	

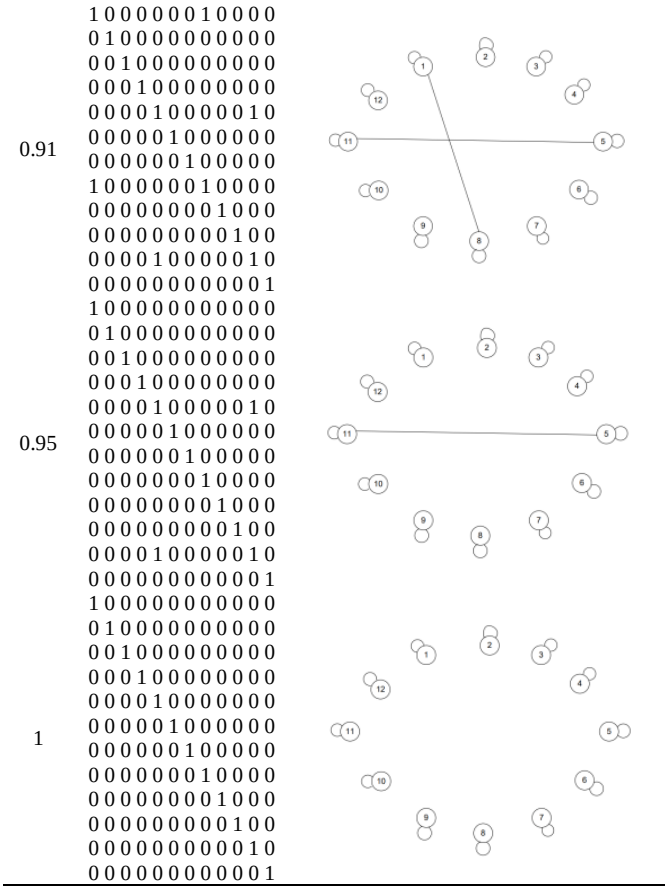


Table 8. Threat classes are equivalent in weight

Level	№	Threat classes
α = 0.76	1	{K1, K2, K3, K4, K5, K6, K7, K8, K9, K10, K11, K12}
α = 0.81	2	{K1, K2, K3, K4, K5, K6, K7, K8, K9, K11, K12}, {K10}
α = 0.84	3	{K1, K2, K3, K4, K5, K6, K8, K9, K11, K12} {K7}, {K10}
α = 0.85	4	{K1, K3, K4, K5, K6, K8, K9, K11, K12} {K2}, {K7}, {K10}
α = 0.86	5	{K1, K4, K5, K6, K8, K9, K11, K12} {K2}, {K3}, {K7}, {K10}
α = 0.87	6	{K1, K4, K5, K6, K8, K9, K11} {K2}, {K3}, {K7}, {K10}, {K12}
α = 0.88	7	{K1, K5, K6, K8, K11} {K2}, {K3}, {K4}, {K7}, {K9}, {K10}, {K12}
α = 0.91	9	{K1, K5, K8, K11} {K2}, {K3}, {K4}, {K6}, {K7}, {K9}, {K10}, {K12}
α = 0.95	11	{ K5, K11} {K1}, {K2}, {K3}, {K4}, {K6}, {K7}, {K8}, {K9}, {K10}, {K12}
α = 1	12	{K1}, {K2}, {K3}, {K4}, {K5}, {K6}, {K7}, {K8}, {K9}, {K10}, {K11}, {K12}

On Figure 1 we will reflect the decomposition tree of the set of threats to information in the cybersecurity system chosen by us for research, the socio-economic system, into non-overlapping equivalence classes. We tried to describe all the calculations in the most accessible and simple way and present them in a form that is understandable to the reader. Figure 1 presented as the result of the study, in our opinion, better copes with the task.

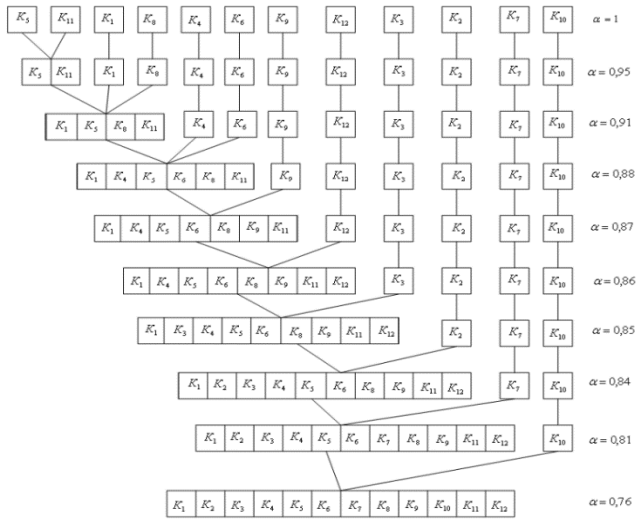


Figure 1. Decomposition tree of the set of information threats in the «Sigma Software» cybersecurity system into equivalence classes

According to the results presented in Figure 1, we can note that with the maximum certainty (which is equal to 1), each information threat in the cybersecurity system constitutes a universal weight cluster. At the same time, taking into account quantitative estimates of the significance of threats, we will choose the level of uncertainty α = 0.95, since it is at this level that all threats do not differ in ranks. At this level of uncertainty, we get: ρ_1=1.89; ρ_2=ρ_6=2.42; ρ_3=ρ_4=2; ρ_7=2.14; ρ_8=2.22; ρ_9=2.25; ρ_{10}=2.2; ρ_{12}=1.33. ρ_5=ρ_{11}=2.61.

At the same time, let S_0 imagine the costs of ensuring the protection of information in the «Sigma Software» cybersecurity system, which are acceptable and possible. In this case, these costs should be divided in proportion to certain ranks of cybersecurity threats (9):

$$\sum S_i=S_0,\ S_1=0.072S_0,\ S_2=S_6=0.093S_0,\ S_3=S_4=0.077S_0,\ S_5=S_{11}=0.1S_0,\ S_7=0.082S_0,\ S_8=0.085S_0,\ S_9=0.086S_0,\ S_{10}=0.084S_0,\ S_{12}=0.051S_0, \quad (9)$$

Otherwise, we denote by λ_0 the level of permissible intensity of the reduction of the information security system «Sigma Software» (10):

$$\sum \lambda_i=\lambda_0,\ \lambda_1=0.072\lambda_0,\ \lambda_2=\lambda_6=0.093\lambda_0,\ \lambda_3=\lambda_4=0.077\lambda_0,\ \lambda_5=\lambda_{11}=0.1\lambda_0,\ \lambda_7=0.082\lambda_0,\ \lambda_8=0.085\lambda_0,\ \lambda_9=0.086\lambda_0,\ \lambda_{10}=0.084\lambda_0,\ \lambda_{12}=0.051\lambda_0, \quad (10)$$

So, the results of the study made it possible to rank the information security threats identified for the article in the cybersecurity system of the object we have chosen («Sigma Software»). It is possible that the ranking results are not quite accurate and have a certain amount of inaccuracy, but along with the above, the main thesis that runs through our study is to demonstrate the effectiveness and efficiency of the presented approaches for solving such problems. In general,

this made it possible to determine the permissible intensity of reducing the level of information security in the Sigma Software cybersecurity system. In addition, the costs of ensuring the security of information in the «Sigma Software» cybersecurity system were also determined. The practical effect will be that this can contribute to the timely introduction of effective mechanisms to counter threats, the rational redistribution of forces and means to neutralize them.

5. DISCUSSIONS

We should discuss the differences between the results of our study and similar ones. Firstly, for example, some scientists [14-16] consider methods for assessing the impact of threats on the level of cybersecurity associated with qualitative, quantitative and mixed assessment of information risks. Highlight their advantages and disadvantages. A number of models are considered for assessing the risks of a cybersecurity system based on fuzzy logic. As a result, it is established that most of the above methods and models require complex calculations and a long time to process the necessary data, while risk assessment is most often carried out only to the level of assets, and their impact on the functioning of the system under study is not taken into account. But our study does not focus on the analysis of all existing methods, but uses one, specific methodological approach for one, specific socio-economic system and its cybersecurity.

Other scientists, in similar studies, propose [17] a model for assessing the level of information security based on a cognitive approach that simplifies calculations and reduces the processing time of incoming information. Others [18] improve the visibility of the input data to ensure cybersecurity protection. Scenario modelling is carried out, as a result of which the level of security of the system itself is determined [19, 20]. However, in our case, the focus is on ranking information threats in the cybersecurity system in order to determine the level of protection and the costs of this.

Discussing the results of the study, one should also talk about the shortcomings. The main disadvantage is that we have chosen only one socio-economic system and its information.

6. CONCLUSIONS

Summing up the results of our study, the ranking of information threats in the cybersecurity system of a single object selected for research was carried out using the theory of fuzzy relations. On the basis of certain ranks, the set of threats is divided into classes that do not intersect and are equivalent to weight. To ensure the security of the systems under study, the distribution of allowable costs in proportion to the ranks of threats is proposed, which will contribute to the rational use of resources and means to prevent, eliminate or reduce the impact of possible cybersecurity threats. In addition, based on the ranking of threats, the permissible intensity of reducing the level of protection of the cybersecurity system was determined, which will allow timely implementation of effective mechanisms to counter threats, rationally redistribute forces and means to neutralize them.

It should be noted that the results obtained allow us to predict the development of the situation in order to make timely and effective management decisions aimed at increasing the security of the information itself in the cybersecurity system. Attention should be paid to determining the influence of the most significant concepts of a fuzzy cognitive map on the security of information as such in the cybersecurity system of the selected object. The results of which make it possible to determine and compare the levels of influence of the studied threats on the security of a given object at different points in time.

REFERENCES

[1] Ilchenko, O.V., Chumak, V.V., Kuzmenko, S., Shelukhin, O., Dobrovinskyi, A.V. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. Journal of Legal, Ethical and Regulatory, 22(2): 6.

[2] Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3): 299-310. https://doi.org/10.18280/ijsse.120304

[3] Yemelyanov, V., Nikonenko, U., Sytnyk, Y., Okhrimenko, I., Shulga, A. (2022). A model for countering the information and technical threats of intellectual capital management of innovation-oriented systems in the engineering sector. Ingénierie des Systèmes d'Information, 27(5): 799-806. https://doi.org/10.18280/isi.270513

[4] Kryshtanovych, M., Filippova, V., Huba, M., Kartashova, O., Molnar, O. (2020). Evaluation of the implementation of the circular economy in EU countries in the context of sustainable development. Business: Theory and Practice, 21(2): 704-712. https://doi.org/10.3846/btp.2020.12482

[5] Kryshtanovych, M., Petrovskyi, P., Khomyshyn, I., Bezena, I., Serdechna, I. (2020) Peculiarities of implementing governance in the system of social security. Business, Management and Education, 18(1): 142-156. https://doi.org/10.3846/bme.2020.12177

[6] Kryshtanovych, S., Lyubomudrova, N., Tymofeev, S., Shmygel, O., Komisarenko, A. (2022). Modeling ways of counteraction to external threats to corporate security of engineering enterprises in the context of COVID-19. International Journal of Safety and Security Engineering, 12(2): 217-222. https://doi.org/10.18280/ijsse.120210

[7] Magruk, A. (2016). Uncertainty in the sphere of the Industry 4.0 – potential areas to research. Business, Management and Economics Engineering, 14(2): 275-291. https://doi.org/10.3846/bme.2016.332

[8] Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. International Journal of Safety and Security Engineering, 11(4): 361-367. https://doi.org/10.18280/ijsse.110409

[9] Lainjo, B. (2020). Network security and its implications on program management. International Journal of Safety and Security Engineering, 10(6): 739-746. https://doi.org/10.18280/ijsse.100603

[10] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20: 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

[11] Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A.

(2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: practical aspect. Business and Economic Horizons, 14(4): 926-940. https://doi.org/10.15208/beh.2018.63

[12] Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. Business: Theory and Practice, 20: 446-455. https://doi.org/10.3846/btp.2019.41

[13] Musman, S., Turner, A.J. (2018). A game oriented approach to minimizing cybersecurity risk. International Journal of Safety and Security Engineering, 8(2): 212-222. https://doi.org/10.2495/SAFE-V8-N2-212-222

[14] Dumchykov, M., Utkina, M., Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. International Journal of Safety and Security Engineering, 12(4): 481-490. https://doi.org/10.18280/ijsse.120409

[15] Leukfeldt, E.R., Lavorgna, A., Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. European Journal on Criminal Policy and Research, 23(3): 287-300. https://doi.org/10.1007/s10610-016-9332-z

[16] Martínez, J., Durán, J.M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5): 537-545. https://doi.org/10.18280/ijsse.110505

[17] Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, 11(1): 101-104. https://doi.org/10.18280/ijsse.110111

[18] Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3): 269-284. https://doi.org/10.1109/JIOT.2015.2460333

[19] Haddon, D.A.E. (2020). Zero Trust networks, the concepts, the strategies, and the reality. Strategy, Leadership, and AI in the Cyber Ecosystem: The Role of Digital Societies in Information Governance and Decision Making, 195-216. https://doi.org/10.1016/B978-0-12-821442-8.00001-X

[20] Tamburri, D.A., Miglierina, M., Di Nitto, E. (2020). Cloud applications monitoring: An industrial study. Information and Software Technology, 127: 106376. https://doi.org/10.1016/j.infsof.2020.106376