Evaluation of Effectiveness of Reduction Information Risk Using Fuzzy Algorithm

Alexander Bolshakov, Ekaterina Rogatneva
MTUCI
Moscow, Russia
as.bolshakov57@mail.ru, swamp.swift@gmail.com

***Abstract*—This article considers the problem of effective risk evaluation in the informational system. Risk evaluation is the main step in the ISMS process. The article uses the standards ISO / IEC 27001 and ISO / IEC 27005. As an example, the threat model formed for the state information system is considered.**

I. Introduction

Today, the vast majority of companies use information systems on a large scale, which increases their dependence on information technology. One of the most important issues for the development of these systems and provision of its stability is security, and the main step in managing information security of an organization is risk evaluation.

Modern Russian companies and organizations are not interested enough in the problem of risk evaluation, and sometimes they are completely indifferent to managing their risks. However, this indifference can lead to drastic consequences, for example, loss of financial assets or leakage of personal data.

There is a positive trend in the number of incidents involving thefts of users' personal data. Usually social networks or state information systems become sources of this kind of data.

Inadequate risk evaluation or complete absence of it can lead to the fact that system developers will not be aware of threats they need to pay attention to. Therefore, the critical vulnerabilities of these threats will remain open to attackers.

In order to make the risk evaluation procedure simple and effective, using of fuzzy logic algorithms is suggested, which at a certain step allow to get rid of strict quantitative assessments and replace them with more intuitive conceptual evaluations.

Such estimates in the theory of fuzzy sets are called linguistic variables. These variables can take phrase values from natural or artificial languages [2].

II. Modeling threats

First step in evaluation of effectiveness of information risk reduction using fuzzy logic algorithm is threat modeling (planning state information system as an example) using expert assessments.

Threat modeling will be held according to FSTEC methodology [1]. Using the indicators of initial security of ISPD, define its technical and operational characteristics, as well as the level of security. In Table 1 "+" means implementation of the requirement of FSTEC for security, "-" means failure to follow these requirements.

1) ISPD has the high level of initial security if not less than 70% of characteristics ISPD correspond to level "high" (positive decisions on the first column appropriate to high level of security), and the others – to the medium level of security (positive decisions on the second column) are summarized.
2) ISPD has the medium level of initial security if conditions on Paragraph 1 are not satisfied and not less than 70% of characteristics ISPD correspond to level not below "medium" (the sum relation positive decisions on the second column appropriate to the medium level of security, to total number of decisions undertakes), and the others – to the low level of security.
3) ISPD has low degree of initial security if not conditions on Paragraphs 1 and 2 are satisfied.

TABLE I. Specifications and level of security of ISPD [1]

Technical and operational characteristics of ISPD	**Security level**		
	High	Medium	Low
By location: local ISPD, deployed within one building	+	-	-
By connection to public networks: ISPD, which has a single point access to the public network	-	+	-
By built-in (legal) operations with personal data database records: recording, deleting, sorting	-	+	-
By the differentiation of access to personal data: ISPD, to which all employees of the organization that owns ISPD have access	-	-	+
By the connections to other databases of PD of other ISPD: ISPD, in which one PD is used, belonging to the organization - the owner of this ISPD	+	-	-
By level of generalization (depersonalization) of PD: ISPD, in which the data provided to the user is not impersonal (there is information that allows to identify the subject of PD)	-	-	+
By volume of PD, which are provided to third-party ISPD users without preprocessing: ISPD, providing part of PD	-	+	-

Based on the data obtained, we will determine the initial level of security and make up a list of actual threats. ISPD has a low degree of initial security, since less than 70% of system characteristics correspond to “high” and “medium” levels. For the compilation of the list of actual security threats for PD of each degree of initial security is assigned a numerical

coefficient Y1. In this case, this coefficient will be equal to 10 [1]. Next, it is necessary to determine the frequency (probability) of the threat realization - this value is determined on the basis of expert estimates. It characterizes the likelihood of a specific threat to the security of personal data for a given PD in specific conditions. According to the method of determination of actual threats of the security of personal data when they are processed in the informational systems of personal data, assessing the probability of a threat may take the following values [1]:

- **unlikely** – there are no objective prerequisites for the threat (for example, the threat of theft of information by persons who do not have legal access to the room where the latter are stored);
- **low probability** – objective prerequisites for the realization of the threat do exist, but the measures taken significantly complicate its implementation (for example, appropriate informational security tools are used);
- **medium probability** - objective prerequisites for the realization of the threat do exist, but the measures taken to ensure the safety of PD are insufficient.;
- **high probability** - objective prerequisites for the realization of the threat do exist and measures to ensure the safety of PD are not taken.

Each linguistic variable is assigned with numerical coefficient Y_2 [1]:

- 0 – for unlikely threat;
- 2 – for low probability threat;
- 5 – for medium probability threat;
- 10 – for high probability threat.

The coefficient of realizability of the threat Y is determined by the following ratio [1]:

$$Y = (Y_1 + Y_2)/20 \quad (1)$$

Based on the value of the coefficient of realizability of the threat Y, the following statements are formed [1]:

- If $0 \le Y \le 0.3$, the possibility of threat is **low**;
- If $0.3 < Y \le 0.6$, the possibility of threat is **medium**;
- If $0.6 < Y \le 0.8$, the possibility of threat is **high**;
- If $Y > 0.8$, the possibility of threat is **very high**.

Then we evaluate the danger of each threat on the basis of a survey of experts and, according to [1], we will define linguistic variables describing the danger to the considered IPDA:

- **Low danger** – the realization of a threat may lead to minor negative consequences for personal data subjects.;
- **Medium danger** – the realization of the threat may lead to negative consequences for the subjects of personal data;
- **High danger** – the realization of a threat can lead to significant negative consequences for personal data subjects.

III. Formation of the rules of fuzzy logic

Formation rules is an important step in building a risk evaluation system that functions on fuzzy logic algorithms. With the help of the rules, the membership functions are build - the characteristic functions, which show the degree each term from the range belongs to a given fuzzy set.

There are two groups of methods for constructing membership functions of a fuzzy set according to expert estimates: direct and indirect [7]. In direct methods, the rules for determining the values of a function are set directly by the expert, and indirect values are chosen in such a way as to satisfy the pre-defined conditions. This paper uses a direct method for constructing membership functions.

Fuzzy logic algorithms imply the use of verbal rule systems. The most common scheme for constructing these rules is the scheme "IF ... THEN ...". These rules are subjective, as they are made up by the experts themselves according to their vision of the problem, experience, and according to certain regulatory documents. In the methodology [1], it is recommended using the combinations shown in Table II.

TABLE II. Expert dependencies of a possibility of realization of threats on degree of danger of threats

The possibility of the threat	**Threat danger indicator**		
	Low	Medium	High
Low	irrelevant	irrelevant	relevant
Medium	irrelevant	relevant	relevant
High	relevant	relevant	relevant
Very high	relevant	relevant	relevant

Usually in any company, three types of information security measures are implemented - at the software-hardware level, at the organizational level and at the engineering-technical level. Based on this, we will define the following linguistic variables accordingly: “Hardware-software protection level” (referred as HsP level), “Organizational protection level” (referred as OrgP level), and Engineering protection level (referred as EngP level). Now let us set a fuzzy scale, which is necessary for obtaining subjective expert assessments. Let's set the following values for each of the protection levels: “Very Low”, “Low”, “Medium”, “Good”, “High” [3]. To establish the correspondence between the values of the fuzzy scale and numerical intervals, we use the psychophysical scale - a function of the likelihood of Harrington [4]. This function is a verbal-numeric scale, and the table below contains the numerical values obtained as a result of statistical analysis of a large array of estimated data obtained during the survey of people. Due to this, the Harrington scale is universal and can be used to evaluate information risks.

TABLE III. FORMATION OF A SCALE FOR RULES OF FUZZY LOGIC

Numerical score	Verbal evaluation	Numeric intervals
1	Very Low	0 – 0.2
2	Low	0.2 – 0.37
3	Medium	0.37 – 0.63
4	Good	0.63 – 0.8
5	High	0.8 – 1

The rule base is a set of all permutations of two (scheme "IF ... And ..., THEN") and three ("IF ... And ... And ..., THEN") elements. A fragment of the rule set is shown in Table IV.

TABLE IV. FORMATION OF RULES OF FUZZY LOGIC

	Level HsP	Level OrgP	Level EngP		Evaluation
	Very Low	Very Low	Very Low		Very Low
	Very Low	Very Low	Low		Very Low
	Very Low	Very Low	Medium		Low
	Very Low	Very Low	Good		Low
	Very Low	Low	Low		Low
	Very Low	Low	Medium		Low
	Very Low	Low	Good		Low
	Very Low	Low	High		Medium
	Very Low	Medium	Medium		Low
	Very Low	Medium	Good		Medium
	Very Low	Medium	High		Medium
	Very Low	Good	Good		Medium
	Very Low	Good	High		Medium
	Very Low	High	High		Good
	Low	Low	Low		Low
If …	Low	Low	Medium	Then	Low
	Low	Low	Good		Medium
	Low	Low	High		Medium
	Low	Medium	Medium		Medium
	Low	Medium	Good		Medium
	Low	Medium	High		Medium
	Low	Good	Good		Medium
	Low	Good	High		Good
	Low	High	High		Good
	Medium	Medium	Medium		Medium
	Medium	Medium	Good		Medium
	Medium	Medium	High		Good
	Medium	Good	Good		Good
	Medium	Good	High		Good
	Medium	High	High		Good
	Good	Good	Good		Good
	Good	Good	High		Good
	Good	High	High		High
	High	High	High		High

As the membership function, we choose a triangular function as the most optimal in the conditions under consideration.

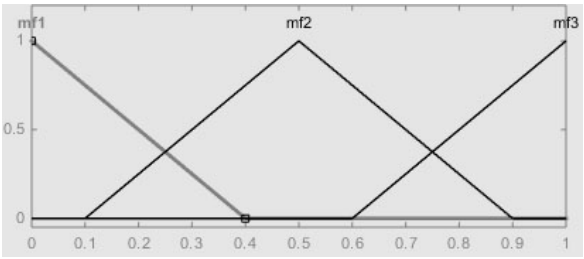

Fig. 1. Triangular membership function

IV. INFORMATIONAL RISKS EVALUATION OF INFORMATIONAL SYSTEM SECURITY

Next step is obtaining expert evaluations. Suppose that experts defined the level of hardware-software protection as “Medium”, the level of organizational protection as “Medium”, and the level of engineering-technical protection as “Good” (Table IV). In this case, the assessment of the level of risk will be equal to the value of “Medium”, and we will get the following graph.

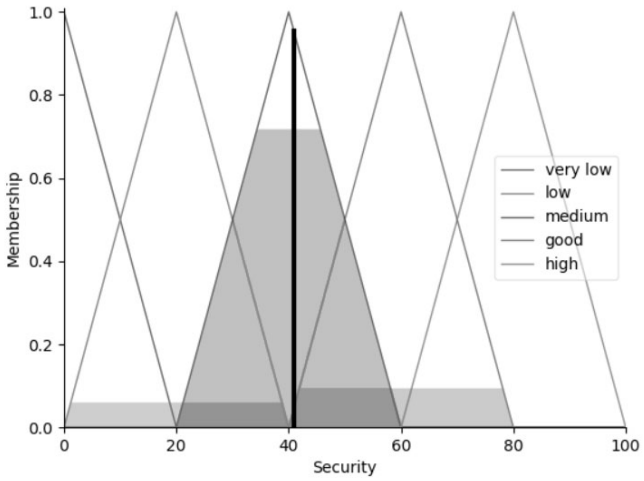

Fig. 2. Aggregated membership and result (line)

To determine the effectiveness of reducing information risk, it is necessary to determine the risk for each protective resource. It is determined by the following formula [6]:

$$R = CThR * D \quad (2)$$

where CThR is the general level of threats by resource, D is the criterion of criticality. CThR is determined by the formula [6]:

$$CThR = 1 - \prod(1-CTh) \quad (3)$$

where CTh is the threat levels for all vulnerabilities, and the number of factors is determined by the number of threats affecting the resource. The CTh value is determined as follows [6]:

$$CTh = 1 - \prod(1-Th) \quad (4)$$

where Th is the threat levels for a particular vulnerability, and the number of factors is determined by the number of vulnerabilities through which the threat is implemented. This parameter is determined by the following relationship:

$$Th = P(V) * ER \quad (5)$$

where P (V) is the probability of the realization of this threat through vulnerability during the year, ER is the criticality of the realization of the threat [6].

Let's agree to measure this value in conventional money units. Let criterion of criticality for software-hardware protection is equal to 15,000 conventional units, for organizational protection - 10,000 conventional units, and for engineering and technical protection - 7,000 conventional units. Also, let the total threat level for a resource be 9.6, 7.06, 6.48 (1), respectively. Then, the risk for the resource of software-hardware protection is equal to 14,400 conventional units, for the resource of organizational protection - 7,060 conventional units, and for the resource of engineering-technical protection - 4,536 conventional units. To reduce the risks we can assume the use of compensatory measures to protect information. The required level of risk will be achieved iteratively according to the requirements [5]. After receiving expert estimates taking into account the application of compensatory measures, for example, the levels are rated, respectively, as "Good", "Good", "Good" (Table IV), the evaluation of the level of risks will be equal to the value of "Good", as seen in Fig. 3.

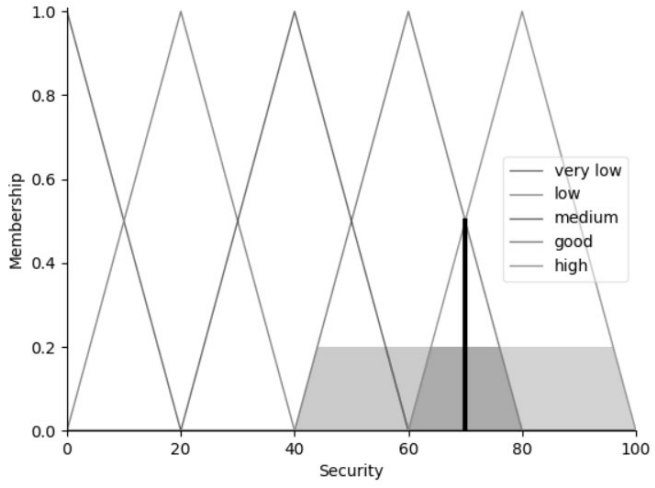

Fig. 3. The state of the system after applying compensatory measures.

As can be seen from Fig.3, the assessment of the level of risks has changed in the direction of "good." This is a positive effect of compensatory measures that need to be evaluated.

V. Evaluation of the efficiency of the protective measures applied

Consider how the indicators have changed after the application of protective compensating measures. The criteria for criticality for all levels will remain the same.

The overall level of threats to resources has changed as follows: hardware-software protection - 2.48 (increase in security is 74%), organizational protection - 2.16 (increase in security is 69%), engineering-technical protection - 6.48 (increase in security is not observed, as the application of compensating measures for this resource was not required). It can be concluded that, on average, the overall level of threats has decreased by 48%. The risk on the resource has also changed - for software-hardware protection it is 3,720 (74% less than before the application of protective measures) conditional units, for organizational protection - 2,160 (69% less) conditional units. The risk for the engineering protection resource has not changed.

Based on the data obtained, compensating measures can be considered quite effective, but their effectiveness is considered only from the side of ensuring the level of information security sufficient for the planning state information system. For a better understanding of how to optimize the risks of an organization, you can use a three-dimensional surface that reflects the dependence of the security level in a company on various expert assessments given by experts in terms of software-hardware protection, organizational protection and engineering-technical protection provided in the company [3].

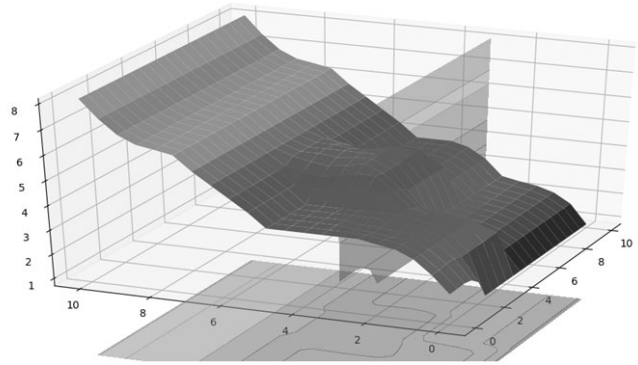

Fig. 4. Simulated three-dimensional surface

On the chart along the X, Y, Z axes, there are estimates of the level of software-hardware protection, organizational protection and engineering-technical protection.

VI. Conclusion

The results obtained during the study allow identifying the interaction of threats, vulnerabilities and related resources and assets necessary for analyzing information risks, as well as allowing to evaluate the effectiveness of reducing information risks using fuzzy logic algorithms. The application of the offered technique can be useful during creation of business processes. The technique is designed to simplify process of

assessment of risk at management of risk of information security.

REFERENCES

[1] Federal Service for Technical and Export Control official website, Methods for determining the actual threats to the security of personal data when they are processed in personal data information systems, Web: https://fstec.ru/component/attachments/download /290.

[2] G.E. Yahyova, *Fuzzy sets and neural networks*. Moscow: BINOM, 2006.

[3] A.S. Bolshakov, E.A. Rogatneva, "Risk assessment of Information Security Using Fuzzy Logic Algorithms", *Telecommunication and Information Technologies*, vol.2, Dec.2018, pp.142-147.

[4] Yu.M. Krakovskiy, *Information Security*. Rostov-on-Don: Feniks, 2017.

[5] Electronic fund of legal and regulatory technical documentation, Information technology -- Security techniques -- Information security risk management, Web: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010.

[6] E.K. Baranova. A.V. Babash, *Information Protection System Modeling*. Moscow: RIOR, 2016.

[7] A.N. Borisov, O.A. Krumberg, I.P. Fedorov, *Fuzzy Model Decision Making: Case Studies*. Riga: Zinatne, 1990.

[8] R. Choudhary, A. Raghuvanshi, "Risk Assessment of a System Security on Fuzzy Logic", International Journal of Scientific & Engineering Research, vol. 3, Dec.2012.