DOI 10.29042/2018-4674-4682

Helix Vol. 8(6): 4674- 4682

Security Risk Assessment Method Using Fuzzy Logic

[1]Ilyas I. Ismagilov, [2]Linar A. Molotov, [3]Timur M. Gilmullin, [4]Igor V. Anikin, [5]Alexey S. Katasev

[1,2] Kazan Federal University

[3]Positive Technologies

[4,5]Kazan National Research Technical University named after A.N. Tupolev

Email: molotov.linar@mail.ru

Received: 02nd November 2018, Accepted: 28th November 2018, Published: 31st December 2018

Abstract

The article solves the problem of assessing security risks in information systems using the methods of the theory of fuzzy sets. The urgency of solving this problem is determined by the complexity of applying a number of existing methods, the possible inaccuracy of quantitative assessments of risk factors, and the possible inadequacy, uncertainty and quality of the initial information. The paper carries out formalization of the subject area "Information Security Risk" in the form of a conceptual model within the framework of the types of ER diagram, and determines the semantics of its concepts within the framework of the theory of categories and factors. The developed methods for assessing information security risks and evaluating the effectiveness of countermeasures are capable of solving problems in the indicated conditions. We have conducted the experiments on the application of the technique on a specific object of protection. The set of countermeasures recommended for implementation shows high efficiency in terms of absolute risk reduction. Recommendations on the choice of forms of membership functions of fuzzy scales used in risk assessment, as well as recommendations on the choice of fuzzy operations when performing calculations are given. The practical application of the developed methodology has a high practical value for building effective information protection systems in terms of expected damage.

Keywords

Information Systems, Information Security, Risk Assessment, Modeling, Conceptual Model, Fuzzy Sets, Fuzzy Logic

Introduction

The modern stage of development of society is characterized by significant changes under the influence of modern information technologies. Currently, intensive research is being conducted in which the attempts to formulate the peculiarities of the impact of Internet technologies, in particular, on the economy are being made.

The digital economics is rapidly replacing the old way of life in almost all spheres of human activity. The expansion of large volume of data, the development of data processing technologies and the tightening of requirements for modern information systems (IS) require their development in many areas. Note the relevance of the task of integration of the IS of organizations with e-commerce systems of various classes [1]. The IS accepted in the process of development should be consistent with the strategy of development of the organization and progress in those areas of informatization methods that play the most important role in the composition of the system. Moreover, decisions often have to be made under the conditions of considerable information uncertainty. Under these conditions, an increase in the level of rationality of the decisions made can be achieved using the methods based on a set-fuzzy approach [2,3].

In the process of developing IS in the conditions of the development of the digital economy, the problem of data security (DS) in organizations is becoming increasingly topical. The specifics of the operation of IS shows constantly growing volumes of threats to DS and damage inflicted on them, which requires adequate counteraction from the standpoint of their security [4]. In modern IS, there are the tendencies of increasing the number of vulnerabilities and vulnerable components [5], which leads to raising requirements for data protection.

Currently, there are two main approaches to the provision of data security in IS:

1) Based on the implementation of the basic level of information security;

2) Based on assessment and management of risks of data security.

The second approach is of particular importance for modern IS, as it enables to build effective information protection systems from the point of view of possible damage, as well as to investigate the economic aspects of the implementation of protective measures [6,7].

Currently, a number of DS risk assessment methodologies are known [8-11]. However, one of their drawbacks is the lack of formal approaches, which form the basis, which does not allow to investigate their relevance, to assess the quality of work. In addition, the use of such methods is complicated by a number of circumstances, one of which is the possible inaccuracy and vagueness of the raw information about the object being assessed.

To analyze the objects and phenomena in the indicated conditions, nowadays, the methods of expert estimation [12] and the theory of fuzzy sets [13-16] are being actively used, which makes their application relevant for solving the problem of data security risk assessment [17-20].

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Methods

There are two approaches to the formation of a conceptual domain model. The descriptive approach involves the task of the subject area by listing all of its objects, listing their properties, highlighting the types of objects, setting the relationship between them and operations. The constructive approach involves the initial setting of object types and the further defining, which objects can be attributed to the specified types. It is preferable to use the second approach for practical purposes.

An approach to the synthesis of the conceptual model of an arbitrary object domain was proposed by P. Chen using the construction of so-called ER-diagrams of object types. Figure 1 represents the upper level of the conceptual model of the subject area "Information Security Risk" in the form of the types of ER-diagram, taking into account the types input, relations and operations.

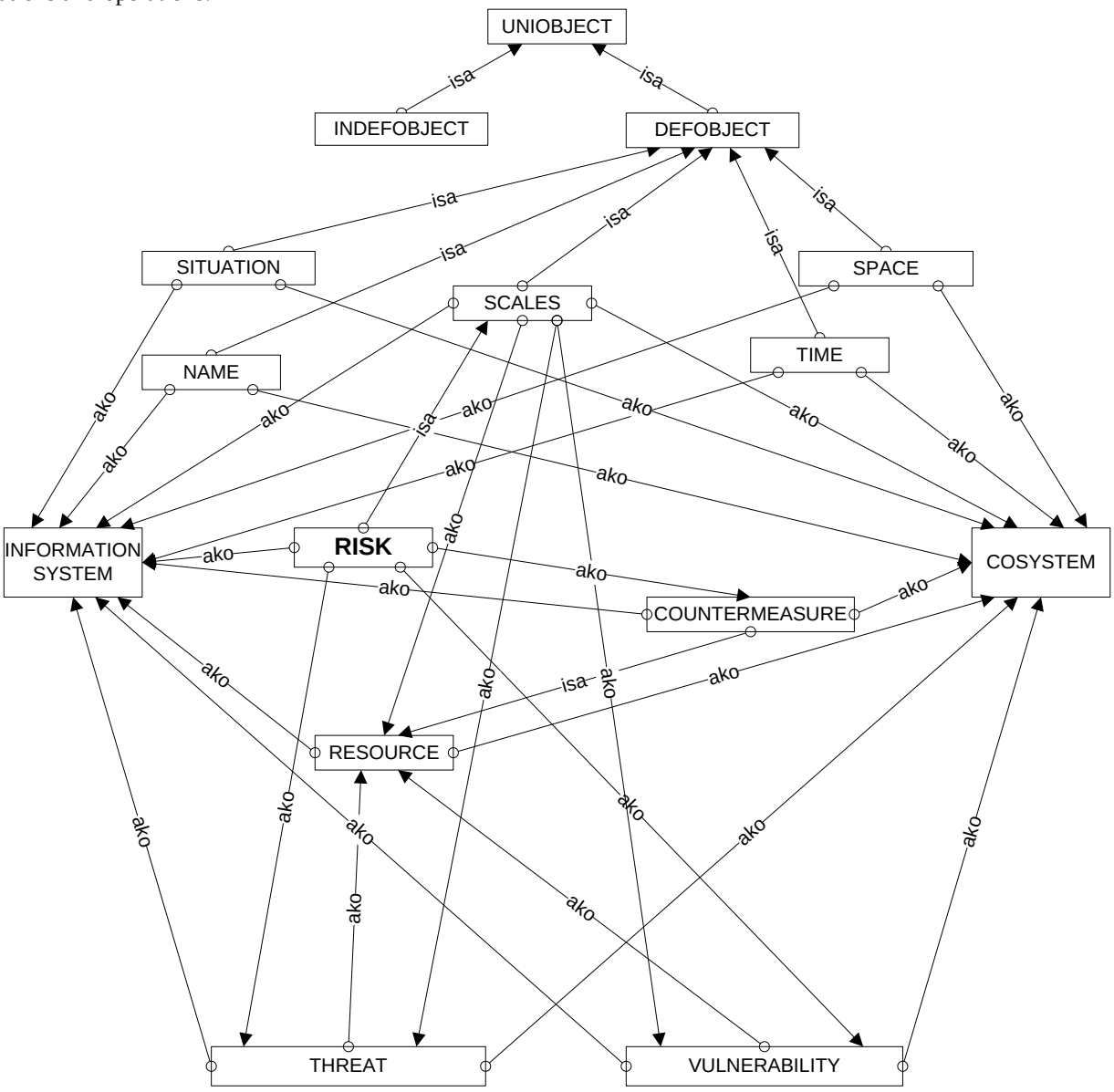

Figure 1: The Upper Level of the Conceptual Domain Model "Information Security Risk"

This diagram includes many types of $t \in Type$ domain objects and the relationships between them. A model of an *INFORMATION SYSTEM* type of the following type is proposed:

$$IS(E) = \{R, T, V, C, Risk, Eff, AllScales, \mathrm{Re}l\}, \quad (1)$$

where $R \subset (t_{\mathrm{Re}c})$ – the set of resources of IS, $T \subset (t_T)$ –the set of threats to IS, $V \subset (t_V)$ –the set of vulnerabilities of IS, $C \subset (t_{CM})$ – the set of countermeasures for IS, *Risk* – the function of risk assessment, *Eff* – the function of evaluating the effectiveness of security measures, *AllScales* – the set of scales for assessing the properties of the elements of IS, *Rel* –the relationship between the elements of IS.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

The resource of $t_{\mathrm{Re}s} \in Type$ is called the type of the objects of IS, satisfying the condition $t_{\mathrm{Re}s}\ ako\ t_{IS} \wedge t_{\mathrm{Re}s}\ ako\ t_{CoSys} \wedge t_{Scale}\ ako\ t_{\mathrm{Re}s}$. To estimate the basic characteristics of the elements of the IS, the following fuzzy measuring scales of t_{Scale} are introduced:

1) confidentiality level (*CL*);
2) integrity level (*IL*);
3) availability level (*AL*);
4) criticality level (*CL*);
5) affect level (*AL*);
6) ease of using vulnerability level (*EL*);
7) risk level (*RL*);
8) damage level (*DL*);
9) opportunity of threat realization level (*OL*);
10) effectiveness countermeasures level (*EffL*).

The result of the evaluation of the properties of the object is determined on a fuzzy scale of the basic characteristics using the basic membership function (MF).

The fuzzy scale of basic characteristics for $t \in Type,\ t \neq t_{Scale}$ – an ordered fuzzy set of $FSBP(t) \in t_{Scale}$ of the vectors *fp*, the coordinates of which are fuzzy basic characteristics of the properties:

$$\forall t \in Type\ \ t \neq t_{Scale}\ \ FSBP(t) \overset{def}{=} \{fp = (fp_i) \mid fp_i \in FP_i\ \ FP_i \in t_{Scale}\} \in t_{Scale}. \quad (2)$$

The basic MF for the objects *e* of $t \in Type,\ t \neq t_{Scale}$ – the membership function of the objects $e \in (t)$ to the vectors of the scale *FSBP*(*t*):

$$bmf : (t) \times FSBP(t) \to [0, 1]. \quad (3)$$

The threat of $t_T \in Type$ – a type of the objects with measurable properties "The potential value of realization of threat", "The preference of the choice of threat by value", "The level of impact of an element", "The level of opportunity of threat realization", satisfying the conditions:

1) $t_T\ ako\ t_{\mathrm{Re}s} \wedge t_{Scale}\ ako\ t_T$;

2) $\forall th \in (t_T)\ \ Risk(IS \cup th) \geq Risk(IS)$.

Vulnerability of $t_{\mathrm{V}} \in Type$ – a type of the objects with measurable properties "The level of influence of the element" and "The level of ease of using vulnerability level", satisfying the conditions:

1) $t_V\ ako\ t_{\mathrm{Re}s} \wedge t_{Scale}\ ako\ t_V$.

2) $\forall th \in (t_T)\ \ \forall v \in (t_V)\ \ Risk(IS \cup (th,\ v)) > Risk(IS)$,

where (*th*, *v*) defines the pair consisting of the threat *th* and vulnerability *v* that realizes it.

The risk $t_{Risk} \in Type$ – a type of the objects measurable on the scale of risks $RS_F \overset{def}{=} \{r \in (t_{Risk}) \mid r \in [0, 1]\} \subset RS$, where $RS = [0, \infty)$ – the space of risks.

The following relations are chosen as the relations *Rel* between the elements of IS.

1. Fuzzy relation of criticality of the resource (*RCR*) – $rcr \subset R \times IS$. To define the criticality of the resource, the function of defuzzification $Critical(r) = Defuz(\mu_{rcr}(r, IS))$ is used.

2. Fuzzy relation of damage induction (*DIR*) – $dir \subset R \times R$. To determine the degree of affect of the element on IS, the function of defuzzification $Affect(r_i, r_j) = Defuz(\mu_{dir}(r_i, r_j))$ is used. Using this relation a tripartite graph (vulnerability – threat – resource) which defines a standard model of threats for IS is given.

3. Fuzzy relation of easiness of using vulnerability (*VEUR*) – $veur \subset V \times T \times R$. To determine the degree of ease of the use of vulnerability, the defuzzification function. $Easy(v_i, t_j, r_k) = Defuz(\mu_{veur}(v_i, t_j, r_k))$ is used.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

A methodology for fuzzy assessment of DP risks and evaluation of the effectiveness of countermeasures in IS (Figure 2) has been developed.

Stage 1. Formation of the IS model.

The expert way is the formation of the IS model in the form (1):

1) ten fuzzy measuring scales are set to assess the basic characteristics of the elements of the IS, as well as their membership functions;

2) the list of elements included in the IS is determined;

3) the properties of the selected elements of the IP are assessed;

4) functions for risk assessment are selected, relations between the elements of the IS are set, fuzzy operations of the composition (T norms and S conorms) are selected.

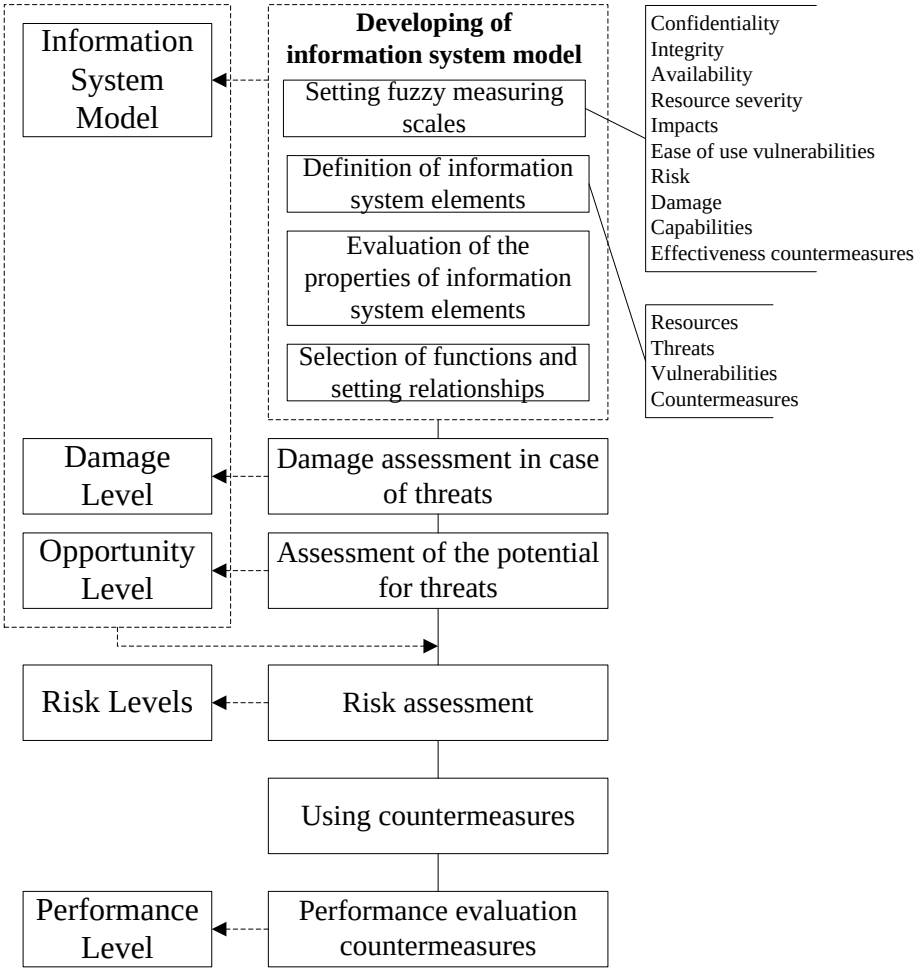

Figure 2: The Diagram of Fuzzy Data Security Risk Assessment and Countermeasure Effectiveness Assessment

A model of relationships between the elements of the IS in the form of the scheme presented in Figure 3 is created.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

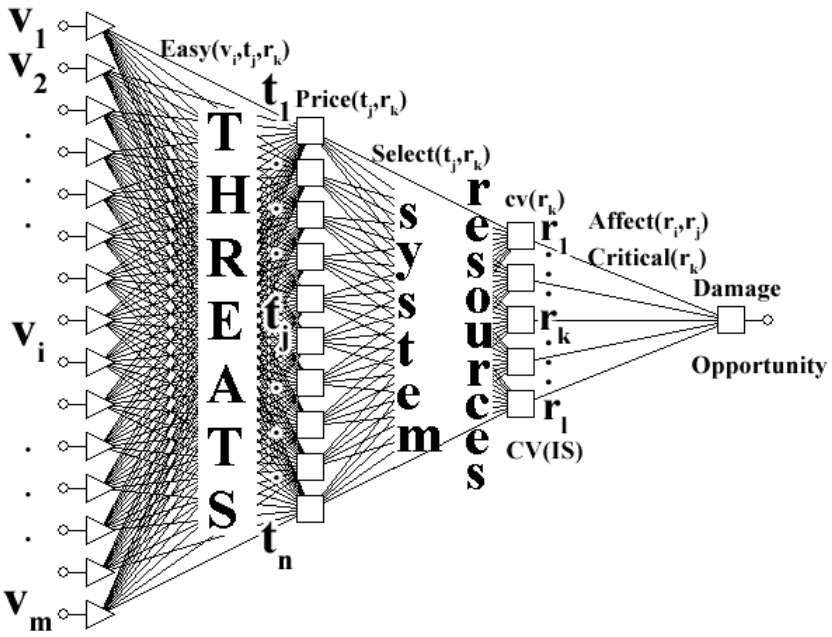

Figure 3: The Scheme of Influence of Threats and Vulnerabilities on the Risk of DS for IS

The main elements of this scheme are the sets of resources, threats, vulnerabilities and countermeasures. When calculating the DS risk level, the defuzzified values of the main risk characteristics of the IS elements are used: criticality values *Critical (r)*, Cost *Cost (r)* and values *Value (r)* of resources, the values of influence *Affect* (r_i, r_j) of resources of r_i on damage of the resources r_j "associated" with him, the values of ease of use of vulnerabilities *Easy (v, t, r)*, the potential cost of realizing threats to the resource *Price (t, r)*.

Stage 2. The assessment of the level of damage to IS in the event of realizing a threat.

We denote by ∘ — the *S*-conorm chosen by the expert for calculating the sum of fuzzy sets, * - the *T*- norm chosen for calculating the product of fuzzy sets. Then, the level of damage to the resource *r* IS is calculated according to (2):

$$Damage(r) = \begin{cases} \sum_k {}^{\circ}(cv(r) * Critical(r) * Affect(r, r_k)), & \text{The absence of counter measures,} \\ Damage(r) * Damage(cm), & \text{The presence of counter measures,} \end{cases} \quad (2)$$

where $cv(r) = \dfrac{Cost(r) + Value(r)}{CV}$ – a relational characteristic "value-cost of the resource" *r*, *Value*(*r*), *Cost*(*r*) – value and cost of the resource *r*, respectively, *CV* – the cumulative value and cost of all resources.

The total degree of damage for IS is calculated according to (3):

$$Damage = \sum_k {}^{\circ} Damage(r_k). \quad (3)$$

If the levels of confidentiality L_C, integrity L_I and availability L_A for the resource have been defined, then the levels of damage by each of the properties are calculated according to (4)-(6), respectively.

$$Damage_C(r) = Defuz(L_C) \cdot Damage(r). \quad (4)$$

$$Damage_I(r) = Defuz(L_I) \cdot Damage(r). \quad (5)$$

$$Damage_A(r) = Defuz(L_A) \cdot Damage(r), \quad (6)$$

where *Defuz* – the function of defuzzification.

The linguistic value *DL* of damage for IS is determined on the fuzzy scale FP_{Damage}.

Stage 3. Assessment of potentiality of realization of threats for IS.

The potentiality of realization of the threat *t* for the resource *r* is defined as

$$Opportunity(t, r) = Select(t, r) * \sum_{i=1}^{m} {}^{\circ} Easy(v_i, t, r), \quad (7)$$

where *Select*(*t*, *r*) – the level of "level preference" by a disrupter of the threat *t* for its realization to the resource *r* from the point of view of resource consuming:

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

$$Select(t, r) = \neg\left(\frac{\Pr ice(t, r)}{\max_j \Pr ice(t_j, r)}\right), \quad (8)$$

where *Price*(*t, r*) – an expert evaluation of preparatory costs of a disrupter needed for him to realize the threat *t* to the resource *r*; *Easy*(v_i, *t, r*) – the level of ease of using vulnerability determined by an expert.

The potentiality of realization of all threats to IS is evaluated according to (9):

$$Opportunity = \sum_{k=1}^{l} {}^{\circ} \sum_{j=1}^{n} {}^{\circ} Opportunity(t_j, r). \quad (9)$$

The linguistic value *OL* of the potentiality of realization of threats to IS is evaluated on the fuzzy scale $FP_{Opportunity}$.

Stage 4. Evaluation of the level of risk of DS.

The general level of fuzzy risk for data security for IS is evaluated according to (10):

$$Risk(IS) = Damage^{*} Opportunity. \quad (10)$$

Having chosen *S*-conorms and *T*-norms, we obtain the concrete values of fuzzy risk for DS.

Stages 5, 6. Introduction of a countermeasure and assessment of its effectiveness.

- absolute estimate of effectiveness:

$$Eff_1(cm.\ IS) = \begin{cases} r_{old} - r_{new}, r_{old} > r_{new}, \\ 0, r_{old} \le r_{new}. \end{cases} \quad (11)$$

- relative estimate of effectiveness:

$$Eff_2(cm,\ IS) = \begin{cases} \dfrac{r_{old} - r_{new}}{r_{old}}, r_{old} > r_{new}, \\ 0, r_{old} \le r_{new}. \end{cases} \quad (12)$$

Based on the formulae (11) and (12), the most effective countermeasures for IS are chosen.

Results and Discussion

Consider the simplest networking IS, schematized in figure 4.

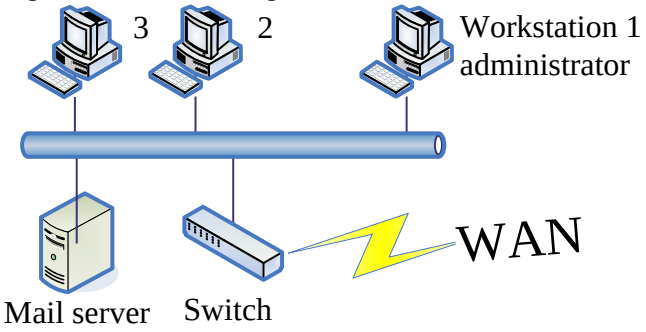

Figure 4: The Scheme of the Simplest Networking IS

The stages of the developed methods for this IS will be the following.

Stage 1. Let use 10 predefined fuzzy scales (see fig. 5).

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

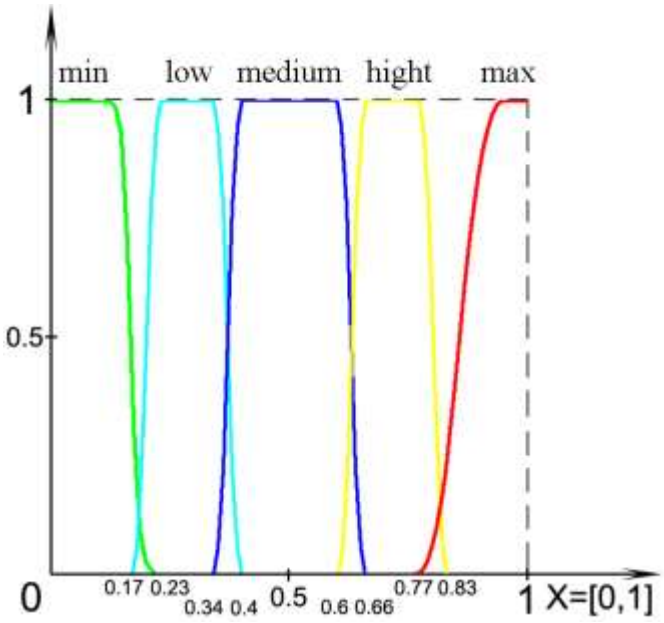

Figure 5: The Membership Functions of Fuzzy Scales "Element Impact Level" and "Vulnerability Simplicity Level"

1. The resources $r_k \in R$, $k = \overline{1,6}$, где r_1 – mail server, r_2 – commutator, r_3 – APM1 of an administrator, r_4 – APM2, r_5 – APM3, r_6 – telecommunications.

2. The threats $t_j \in T$, $j = \overline{1,7}$, where t_1 – an acquisition by the violator of an unauthorized physical access to the IS elements, t_2 – an acquisition by the violator of an unauthorized remote networking access to the IS elements, t_3 – an unauthorized modification of information in mail system, t_4 – a compromise of pass keys to mail server by the establishment of an organization, t_5 – the remote DoS-attacks on the IS elements, t_6 – a fail in networking setup of the IS elements, t_7 – destruction of the resources.

3. The vulnerabilities $v_i \in V$, $i = \overline{1,9}$ in the form of absence v_1 – of regulation of access to the room with resources, v_2 – of the systems of resources observation, v_3 – of the authorization for inputting the changes into the system of e-mail, v_4 – of the rules of working with the system of cryptographic protection of the electronic mail, v_5 – of the agreements with the collaborators on the privacy preserving of key information, v_6 – of concrete management of key information between several collaborators, v_7 – of a hardware firewall, v_8 – of the intrusion detection system to APM1 of an administrator, v_9 – of antivirus and antispyware program in IS.

4. The countermeasures $c_q \in C$, $q = \overline{1,8}$, where c_1 – establishing the policy of security of an organization, regulating the rules of physical and network access by the collaborators to the IS resources, c_2 – introducing the system of physical control and demarcation of the access by means of the system of electronic permit, c_3 – introducing the infrastructure of public keys to demark the network access to the IS resources, c_4 – an obligatory signing by the collaborators of an agreement on privacy preserving of key information, c_5 – installing the commutator with hardware firewall, c_6 – installing the system of intrusion detection system to APM administrator, c_7 – installing an antivirus and antispyware program into IS, c_8 – physical defense of IS by independent security service.

Figure 6 schematically illustrates the directions of "impact" of the IS elements and relations between them, as well as the countermeasures for the IS.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

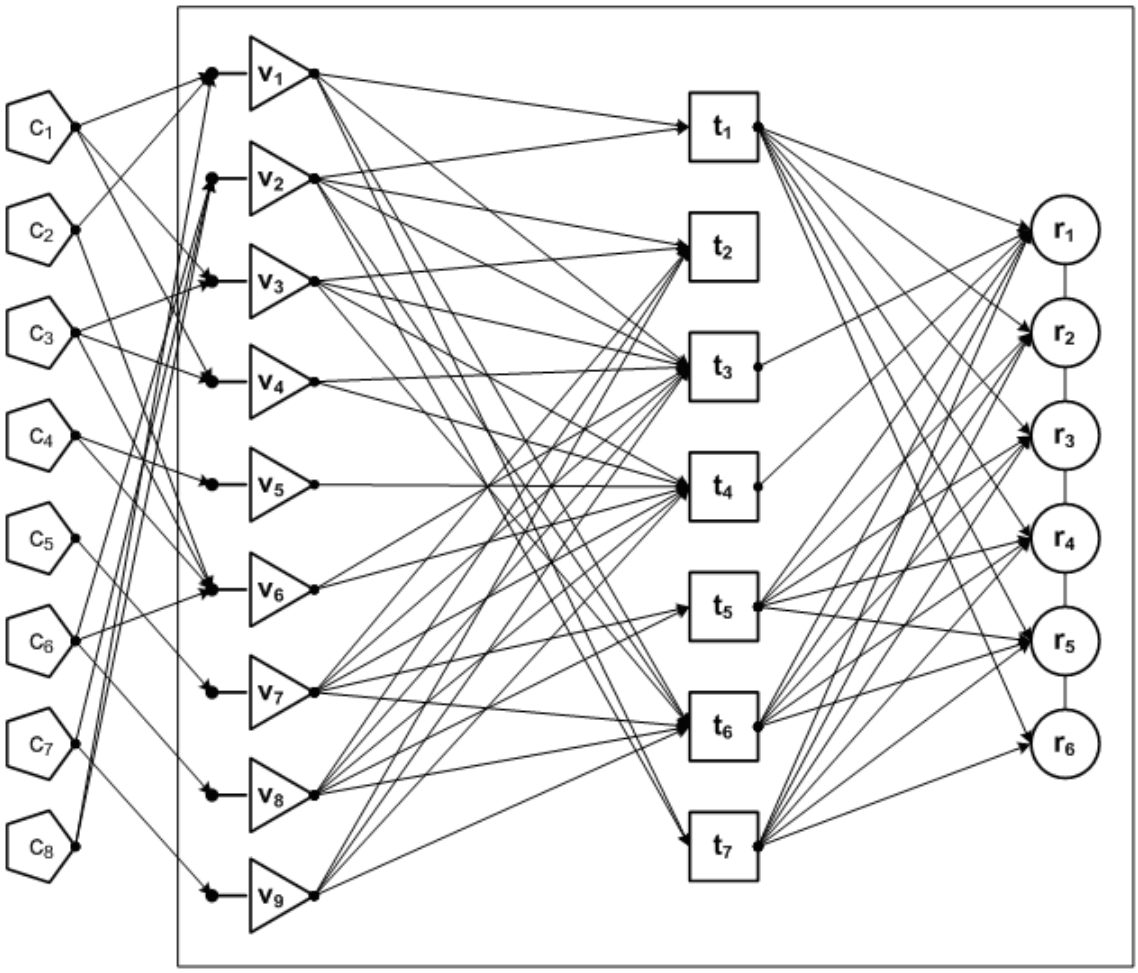

Figure 6: The Scheme of Influence of the IS Elements of Organization

Stage 2. With pessimistic estimation: *Damage*=0.91, *DL=Max*. With optimistic estimation: *Damage*=0.71, *DL*=High.

Stage 3. With pessimistic estimation *Opportunity*=1, *OL=Max*. With optimistic estimation: *Opportunity*=1, *OL=Max*.

Stage 4. The general level of fuzzy risk of DS for IS is calculated according to the formula (10). Pessimistic risk estimation: *Risk*(*IS*)=0.91, *RL=Max*. Optimistic risk estimation: *Risk*(*IS*)=0.71, *RL*=High.

Stages 5, 6. After estimation of the effectiveness of each countermeasure it has been defined that the effectiveness of the totality of countermeasures calculated by the formula (11), despite a relative expensiveness of each of the countermeasures is rather high ($Eff_1(c, IS)$=0.45) and is recommended to realization into organizations.

Summary

As a result of the experimental studies, the following recommendations can be given for the further application of the developed methods:

1) to use smoother forms of membership functions to define fuzzy levels;

2) to use the operations of algebraic product and algebraic sum to reduce the vulnerability of the results of risk assessments when changing the source data.

Conclusion

Risk assessment of information security of IS is an urgent task and requires the development of formal approaches to its solution. This article formalized “Risk B <” subject area as a conceptual model within the types of ER-diagram, and also defined the semantics of its concepts within the framework of the theory of categories and functors. The developed methodology for assessing the risks of data security and evaluating the effectiveness of countermeasures is capable of solving the problems in the context of fuzziness of the initial information. Experiments on the application of the developed methods on a specific object of protection were carried out. At the same time, the set of countermeasures recommended for implementation showed high efficiency in terms of absolute risk reduction. Recommendations on the choice of forms of the membership functions of fuzzy scales used in the risk assessment, as well as on the choice of fuzzy operations when performing calculations, were given. The practical application of the developed methodology has a high practical value for building effective systems of information protection in terms of expected damage.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Acknowledgements
The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. This work was supported by the Russian Federation Ministry of Education and Science, project № 8.6141.2017/8.9.

References

[1] Ismagilov I.I., Belov A.I. Methodological aspects of choosing a portfolio of projects on integration of corporate information systems with e-commerce tools // Kazan Economic Vestnik. – 2010. – Vol.21, Is.4. – P. 64-69.
[2] Ismagilov Ilyas I., Khasanova Svetlana F., Zinov'ev Pavel A., Complex engineering systems: rational choice of evolutionary projects // REVISTA PUBLICANDO. - 2018. - Vol.5, Is.16. - P.409-420.
[3] Katasev A.S., Kataseva D.V., Emaletdinova L.Yu. Neuro-fuzzy model of complex objects approximation with discrete output // 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016.
[4] Anikin I.V. Information security risks assessment in telecommunication network of the university // Proceedings of 2016 International Conference on Dynamics of Systems, Mechanisms and Machines, Dynamics 2016.
[5] Anikin I.V. Using fuzzy logic for vulnerability assessment in telecommunication network // Proceedings of 2017 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017.
[6] Anikin I.V., Emaletdinova L.Yu. Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation // Proceedings of 8th International Conference on Security of Information and Networks, SIN 2015.
[7] Anikin I.V. Information security risk assessment and management method in computer networks // Proceedings of 2015 International Siberian Conference on Control and Communications, SIBCON 2015.
[8] Alberts C., Dorofee A. Managing information security risks. The OCTAVESM approach. Addison Wesley, 2002, 512 pp.
[9] Peltier T.R. Information Security Risk Analysis, third ed., Auerbach Publications, 2010, 456 pp.
[10] Karabacaka B., Sogukpinar I. ISRAM: information security risk analysis method // Computers app. Security, vol. 24, 2005. - P. 147-159.
[11] Shamala P, Ahmad R., Yusoff M. A conceptual framework of info structure for information security risk assessment (ISRA) // Journal of Information Security and Applications, Volume 18, Issue 1, July 2013. – P. 45-52.
[12] Katasev A.S., Kataseva D.V. Expert diagnostic system of water pipes gusts in reservoir pressure maintenance processes // 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016.
[13] Anikin I.V., Zinoviev I.P. Fuzzy control based on new type of Takagi-Sugeno fuzzy inference system // Proceedings of 2015 International Siberian Conference on Control and Communications, SIBCON 2015.
[14] Anikin I., Zinoviev I. New type of Takagi-Sugeno fuzzy inference system as universal approximator // Applied Mechanics and Materials, Volume 598, 2014. – P. 453-458
[15] Ismagilov I.I., Khasanova S.F. Short-Term Fuzzy Forecasting of Brent Oil Prices // Asian Social Science, 11(11). – P. 60-67.
[16] Zadeh L.A. Fuzzy Sets // Information and Control, vol. 8, 1965. – P. 338–363.
[17] Makarevich O., Mashkina I, Sentsova A. The method of the information security risk assessment in cloud computing systems // Proceedings of the 6th International Conference on Security of Information and Networks (SIN'2013), Pages 446-447, 2013.
[18] Joshi C., Singh U.K. Information security risks management framework – A step towards mitigating security risks in university network // Journal of Information Security and Applications, Volume 35, August 2017. – P, 128-137.
[19] Newcomb E.A., Hammell R. FLUF: Fuzzy logic utility framework to support computer network defense decision making // Annual Conference of the North American Fuzzy Information Processing Society – NAFIPS.
[20] Buldakova T.I., Mikov D.A. Comprehensive approach to information security risk management // CEUR Workshop Proceedings Volume, 2017. – P. 21-26.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495