Construction of Membership Functions for Fuzzy Management of Security Information and Events

Igor Kotenko and Igor Parashchuk

Abstract The object of the research in the chapter is the decision-making processes in special security information and event management (SIEM) systems designed for (near) real-time analysis of security threats to modern cyber-physical systems. Some mathematical methods for constructing a membership function as applied to decision-making problems within the framework of fuzzy management of security information and events of cyber-physical systems are studied. The values of the membership function are determined for the decision-making problems on whether a particular computer attack belongs to a fuzzy set of dangerous attacks (a set of attacks of a high level of danger). We consider fuzzy algorithms for solving this problem using a variant of constructing membership functions according to a probabilistic scheme and a method based on the representation of membership functions as functions of the probability density of clear random boundaries between terms of a linguistic variable. At the same time, both the method of constructing membership functions based on the analysis of probability density functions and the method using a simple probabilistic scheme, do not have high mathematical and computational complexity but allow taking into account the uncertainty (fuzziness) of the observed and controlled security parameters, which provides an increase in the reliability of control for security information and events within the framework of security fuzzy management for systems of this class.

Keywords Cyber-physical system · Security information and event management system · Membership function · Fuzzy control · Probability · Computer attack · Security parameters · Threats

I. Kotenko (✉) · I. Parashchuk
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, St. Petersburg 199178, Russia
e-mail: ivkote@comsec.spb.ru

I. Parashchuk
e-mail: parashchuk@comsec.spb.ru

A. G. Kravets et al. (eds.), *Cyber-Physical Systems: Intelligent Models and Algorithms*, Studies in Systems, Decision and Control 417,
https://doi.org/10.1007/978-3-030-95116-0_8

1 Introduction

Unlike classical controlled engineering systems, for example, systems of mechanical engineering, energy, and industrial production, modern cyber-physical systems (CPSs) are large and multicomponent engineering objects implemented based on seamless integration of computational algorithms and embedded physical components. The use of CPSs allows increasing the adaptability, scalability, fault tolerance, and security of engineering systems, as well as the ergonomics (convenience) of their use. It is generally accepted that in systems of this class, the cybernetic and physical components are closely integrated at all scales and all levels within a single information space using sensors and sensors.

CPSs allow organizational and technical interconnection of heterogeneous discrete and continuous subsystems, objects, and processes, integrate the cybernetic component, computer hardware, and software technologies. Within the framework of the CPS, forces, means and processes are combined. These systems are based on the integration of cyber, technological, physical (resource), and information spaces. In other words, these are systems in which resources, technologies, computing elements, and elements of physical nature are interconnected, serving as both consumers and sources of information. The process of functioning of the CPS is based on the exchange of information, therefore, an important area of research—the management of events and incidents of information security—continues to be relevant.

For this purpose, special systems for managing security information and events (Security Information and Event Management, SIEM) are being created, designed to analyze in real-time security events (threats) emanating from network devices and applications, and allowing one to respond to these events (threats) in near real-time. Their task is to prevent significant damage to the integrity, confidentiality, and availability of data [1]. The tasks that SIEM systems solve are as follows: collecting, summarizing, and storing event logs and other security information from a variety of heterogeneous sources; automatic notification and visualization of warnings; use of tools for analysis of incidents and event analysis; analysis and processing of events using data mining methods; preparation of data for investigations (forensic).

The main advantage of SIEM systems is the detection of security threats and attacks at the early stages of their manifestation. In addition, SIEM systems provide forecasting of the behavior of CPSs in the course of a negative impact, which allows the timely development of adequate measures to counter attacks [1, 2].

The processes for monitoring and managing security events and incidents implemented in modern SIEM systems have a complicated hierarchy. But they are traditionally based on decision-making and decision support procedures. The procedures and algorithms for decision-making and its support for the management of security information and events are aimed at implementation at all stages of collecting and analyzing data from digital network content control systems to detect and counteract CPS security threats. At the same time, the tasks of collecting and processing data on security events from distributed sensors, tasks of processing big

data for preliminary analysis of security events, and tasks of assessing security and many others are solved [1–3].

At the same time, the analysis of restrictions on data reliability for making such decisions and solving the listed problems leads to the need to search for a sufficiently rigorous analytical description of the process of developing control actions in a fuzzy environment. In our opinion, these constraints can be taken into account most correctly within the framework of fuzzy control methods considered in several modern works [4–25]. In these works, it is noted that one of the modern approaches to the implementation of such tasks, to obtaining adequate and reliable results of processing big data arrays, the results of decision-making and its support, are the methods and algorithms of fuzzy control.

The chapter proposes the fuzzy algorithms of construction of membership functions for fuzzy management of security information and events and the method for the representation of membership functions as functions of the probability density of clear random boundaries between terms of a linguistic variable. These results allow taking into account the fuzziness of the observed and controlled security parameters, which provides an increase in the reliability of control for security information and events within the framework of security fuzzy management.

The chapter is organized as follows. The related work is outlined in the second section. The algorithms for constructing membership functions of fuzzy sets are suggested in the third section. The method for constructing membership functions based on the analysis of functions of probability density and discussion are considered in the fourth section. The fifth section is the conclusion and plans for further research.

2 Related Work

Technological and methodological approaches used in solving the problems of security management and decision-making on security information and event management are known. The work [3] is devoted to the problems of developing procedures for making such decisions. The proposed algorithms for making decisions on the control and management of information security differ in approach, depth of analysis, and set of controlled parameters. However, the methodological approaches and decision-making algorithms considered are complex from the point of view of mathematical implementation and are not unified for various specific decision-making processes. They are not able to take into account the uncertainty (fuzziness) of the observed and controlled parameters during decision-making. They are not adapted to the tasks of the so-called fuzzy control.

The work [4] considers the issues of fuzzy identification of systems and its application to modelling and control. Here, a generalized management model is proposed in abstract terms, which does not allow it to be fully used to develop control actions to identify specific threats and prevent them within the SIEM framework.

In [5–7] it is argued that fuzzy control algorithms can be implemented using the results of the analysis of a variety of expert opinions. But these algorithms require

significant expenditures for collecting statistics of the initial data that characterize large amounts of expert knowledge. This knowledge serves, in turn, to identify the states of parameters and security indicators in the interests of the efficient operation of SIEM systems. Such approaches to the construction of fuzzy control algorithms will not be able to meet the user's needs for unification and usability (simplicity) of use; they are complex in terms of describing large amounts of expert knowledge.

Thus, in [8–11], applications are proposed for control procedures based on fuzzy clustering algorithms, or on algorithms for constructing "decision trees". But the methods used in these works for determining the membership functions of fuzzy sets are ineffective and not always reliable due to the need to collect and process a set of related data, which is not always possible in practice.

There are known approaches to solving fuzzy control problems and formulating membership functions based on aggregation (geometric and non-geometric) functions [12, 13]. But these approaches are focused mainly on the intuitionistic fuzzy set, which contains both the membership function and the function of non-membership of some arbitrary element in the fuzzy set. For such sets, intuitionistic indices of fuzziness are determined, which does not quite correspond to the tasks faced by SIEM. The work [14] develops the theory of intuitionistic fuzzy sets. This work is devoted to the so-called Pythagorean fuzzy sets, not directly related to the Pythagorean theorem, but using the postulates proved by Pythagoras (including operations with complex numbers) in the formulation and search for membership functions. This method is not bad for analyzing aggregation of satisfaction with criteria and for comparing alternatives, but the formulation of membership functions for solving control problems based on Pythagorean fuzzy algorithms is difficult and time-consuming.

The works [15, 16], as well as, in part, the work [9], analyze and propose to use control algorithms taking into account unreliable initial data. This data can be identified based on the mathematics of fuzzy sets and artificial neural networks. At the same time, the use of such an approach for solving the problems analyzed in our chapter is redundant and requires large computational and time costs (for building and training a neural network).

In [17, 18] an approach to solving problems of fuzzy control and finding values of membership functions based on probabilistic analysis is considered. But this approach is not always accurate, uncontested, does not take into account the values of the probability density functions.

In [19, 20] an interesting approach to the practical application of the algorithms for processing fuzzy sets in problems related to risk management is suggested. Fuzzy risk analysis is simple, accessible, but does not cover the entire range of problems arising in the management of the security information and events (threats) for complex CPS.

The papers [21, 22] are devoted to the possibilities of mathematical descriptions of control processes based on fuzzy logic. Such approaches will be considered in our chapter, these will be options for constructing membership functions of fuzzy sets used in the problems of security information and event management. They are the basis for fuzzy control, but these works do not consider specific management decisions taking into account the values of the probability density. For example, they do not consider the probability density for the lower and upper thresholds for

a particular variable to belong to the entire set of variables, by changing which information and security events are controlled.

The approach considered in [23] is partially free of these shortcomings. However, the fuzzy control model proposed in this work, although it is based on membership functions determined based on alternative identification methods, taking into account uncertainty, is focused on the development of managerial decisions in conditions of local stationarity.

The closest (in physical and mathematical essence) to the idea proposed in this chapter are the papers [24] and [25], where several interacting and complementary approaches to identifying membership functions in the interests of fuzzy management of security information and events are proposed.

Thus, the analysis of related works shows that fuzzy control algorithms are highly versatile, and the combination of simple probabilistic methods for constructing membership functions with methods for their identification based on the analysis of probability density functions opens up ample opportunities for the study of such complex processes as security information and event management.

In other words, it is possible to recognize the unconditional relevance, as well as to assume the theoretical significance and practical possibility of solving the problem of formulating new approaches to decision-making on fuzzy management of security information and events, based on algorithms for constructing membership functions of fuzzy sets.

3 Theoretical Part

Let us consider algorithms for constructing membership functions of fuzzy sets as applied to decision-making tasks for security information and event management. Let us say that the terms of a fuzzy linguistic variable are introduced, i.e. qualitative (not quantitative) values of the logical–linguistic variable x, which characterizes the fuzzy judgments (opinions) of experts and decision-makers, for example, about the current level (degree) of the danger of a particular attack type in CPS: "the level of danger of a particular attack type x is small" and "the severity level of a particular attack type x is large".

It is obvious that any membership function $\mu(x)$ characterizing (within the framework of making a decision on security information and event management) the current level of danger of a particular attack type for the CPS security is subjective. Although it can reflect the opinion of not one person, a whole team or a group of experts.

To make an informed decision on security information and event management, it is necessary to determine the value of the membership functions characterizing the level (degree) of the danger of a particular attack type. One of the simplest fuzzy algorithms for solving this problem is a variant of constructing membership functions according to a probabilistic scheme [24]. The essence of this approach is as follows. Each of the n experts is supposed to answer the question of whether the variable x

belongs to the set A – the set defining the term "high level of danger of a particular attack type for the CPS security". If n1 experts answer the question in the affirmative, and $n2$—in the negative, then they consider that

$$\mu(x) = \frac{n_1}{(n_1 + n_2)}, \tag{1}$$

and $n1 + n2 = n$.

There are more complex algorithms, theoretical principles, and practical procedures for constructing membership functions.

Sometimes important concepts of the norm and universal scale are introduced. These theoretical calculations show that set-theoretic operations (identification of membership functions based on a probabilistic set of operations on fuzzy sets) are correct only when membership functions are measured on a scale of relations. If the measurements are performed only in the order scale, then the operations of identification of membership functions based on the minimax will be correct.

There are four basic classification features of algorithms (methods) for constructing membership functions of fuzzy sets [24]: the assumed form of the domain of definition of a fuzzy set—numeric, including discrete (a) or continuous (b), and non-numeric (c); the method of expert survey used—individual ($d1$) or group ($d2$); type of used expert information—ordinal ($e1$) or cardinal ($e2$); interpretation of expert survey data—probabilistic (D) or deterministic (N).

The basic theoretical methods for constructing membership functions often include an algorithm of the type $< a, d1, e2, N >$. It is based on a quantitative comparison of the degrees of belongingness by an individual decision-maker.

So, for problems with the participation of an individual decision-maker, an algorithm of the type $< b, d1, e2, N >$ is proposed. It is an algorithm for the parametric determination of the membership function of fuzzy sets. Following this algorithm, the form of the function is set axiomatically, and its parameters are directly estimated by the decision-maker. For example, for the case of a triangular shape of the membership function, the decision-maker indicates its parameters u_1, u_2, u_3, at which it takes on the unit and zero values, i.e.

$$\mu_{\tilde{A}}(u_2) = 1, \tag{2}$$

but for all $u \leq u_1$, $u \geq u_3$ there is

$$\mu_{\tilde{A}}(u) = 0. \tag{3}$$

It should be noted that the parametric representation of the membership functions is compact and provides ease of constructing them in practice. At the same time, such a parametric representation of membership functions is associated with the study (and

proof) of the adequacy of the forms used (triangular, trapezoidal, bell-shaped, etc.) and the corresponding analytical descriptions of such membership functions.

A similar approach is used in algorithms based on the use of a standard set of graphs of membership functions. The decision-maker chooses the most suitable graph from the standard set, and then, in a dialogue with the computer, finds out the parameters of this graph and, if necessary, corrects them.

In addition, methods of psychological scaling can also be used to construct membership functions of fuzzy sets. There is an algorithm for constructing membership functions based on the procedure $< b, d1, e2, N >$ and focused on calculating the terms of a linguistic variable with a numerical domain based on the equal division method. In this case, the decision-maker is presented with several pairs of points in turn. At each presentation, the decision-maker must name a point for which the degree of membership is in the middle between the degrees of membership of the points included in the presented pair.

One of the most commonly used fuzzy algorithms for constructing membership functions also belongs to the class $< b, d_1, e_2, N >$. It is based on the representation of membership functions as functions of the probability density of clear random boundaries between the terms of a linguistic variable.

The theoretical analysis of the considered methods allows us to hypothesize that effective approaches to the construction of membership functions in decision-making problems for security information and event management can be found by combining simple probabilistic methods (according to a probabilistic scheme) and a method for constructing membership functions based on the analysis of functions of the probability density. To test this hypothesis, it is proposed to consider the methodological (practical) application of this approach (method) in more detail.

4 Methodological Part and Discussion

Let us consider an algorithm for constructing membership functions based on the analysis of functions of probability density as applied to decision-making problems for security information and event management, for example, to the problem of decision-making about belongingness of a particular computer attack to a fuzzy set of dangerous attacks (a set of attacks of a high level of danger).

Let some set A have the physical meaning of the term of the set of values of the linguistic variable "high level of danger of a particular attack type for information security" and is described by an interval (γ_1, γ_2).

In this case, if object x is the level of danger of a particular attack type $x > \gamma_1$ and $x < \gamma_2$, then $x \in A$, otherwise $x \notin A$.

If γ_1 and γ_2 are random variables, then A is a fuzzy set˜, since there are objects (values of the danger level) x, relative to which it is impossible to unambiguously assert whether they belong to the set A (the set of a high danger level) or not.

Let $f_1(\gamma_1)$ and $f_2(\gamma_2)$ be the probability density functions for the lower and upper thresholds of membership of the variable x (the value of the danger level) to the

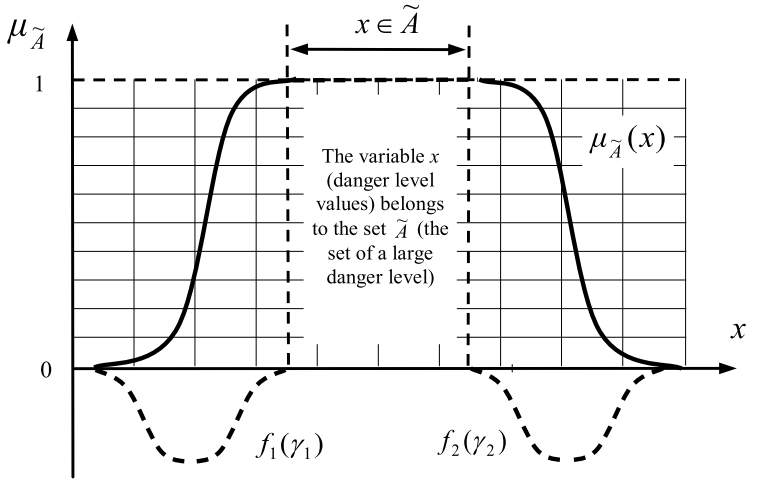

Fig. 1 Graphical interpretation of the construction of the membership function

set A (the set of the high danger level), respectively (Fig. 1). With a probabilistic interpretation of the membership function, we have.

$$\mu_{\tilde{A}}(x) = P(x \in A). \tag{4}$$

Taking into account the introduced notation, we obtain.

$$\mu_{\tilde{A}}(x) = P(\gamma_1 < x < \gamma_2). \tag{5}$$

With the independence of random variables γ_1 and γ_2, we find the value of the membership function for our decision-making problem on whether a particular computer attack belongs to a fuzzy set of dangerous attacks (a set of attacks of a high level of danger).

$$\mu_{\tilde{A}}(x) = P(x > \gamma_1)\ P(x < \gamma_2). \tag{6}$$

We denote by $F_1(x)$ (see Fig. 1) the probability measure (boundaries).

$$F_1(x) \Leftrightarrow \int_{-\infty}^{x} f_1(\gamma_1)\, d\gamma. \tag{7}$$

and by $F_2(x)$–the probability measure (boundaries)

$$F_2(x) \Leftrightarrow \int_{-\infty}^{x} f_2(\gamma_2)\, d\gamma \tag{8}$$

By definition $F_1(x) = P(\gamma_1 < x)$.

Then we get the final value of the membership function for the decision-making problem within the framework of fuzzy management of security information and events—does a specific computer attack of level x belong to a fuzzy set˜of dangerous attacks (a set of attacks of a high level of danger): $\mu_{\tilde{A}}(x) = F_1(x)\,[\,1 - F_2(x)\,]$.

The further development and modification of this approach is an algorithm for the simultaneous determination of membership functions of all basic terms of a linguistic variable based on a survey of a group of experts—the type of the technique $< b, d2, e1, D >$.

In essence, it is an interactive software system for constructing membership functions in terms of linguistic variables based on the considered methods and requirements for a set of such functions.

This approach implies the construction of membership functions in a dialogue mode with a computer-based on the use of a standard set of graphs of membership functions. When implementing this approach, it is necessary to observe some rules that must be followed: the terms of the set T (x) must be ordered; membership functions of extreme terms should not have the form of bell-shaped functions; each term (concept) must have at least one typical object, i.e.

$$\exists\, x_i : \mu_{\tilde{A}}(x_i) = 1. \tag{9}$$

for any two terms, the condition

$$0 < \max_x \mu_{\tilde{C}_i \cap \tilde{C}_j}() < 1 \tag{10}$$

is true, where $\tilde{C}_i$ and $\tilde{C}_j$ are fuzzy sets, the intersection of which gives us the values of the compatibility function.

In other words, at least one concept ($\mu\ (x) > 0$) corresponds to each x, and no compatibility function can be completely nested in another compatibility function of a given linguistic variable.

Thus, using the method of representing membership functions as functions of the probability density of clear random boundaries between the terms of a linguistic variable, as well as based on a standard set of graphs of membership functions, it is possible to obtain the values of these functions, for example, for the statement "the value x is small". The meaning of this statement for our practical task is to determine the current level (degree) of the danger of a particular attack type for the CPS information security—"the level of danger of a particular attack type x is small". To determine the current level (degree) of the danger of a particular attack type for

the CPS information security—"the level of danger of a particular attack type x is large"—the problem of finding membership functions is solved similarly.

5 Conclusion

The considered method shows that it is possible to determine membership functions in such decision-making problems within the framework of fuzzy management of security information and events, not only with the help of procedures for direct questioning of experts but also based on distribution functions $F_1(x)$ and $F_2(x)$ with further use of the expression obtained for $\mu_{\tilde{A}}(x)$. Moreover, the functions $F_1(x)$ and $F_2(x)$ themselves can be built based on either statistical data or an expert survey. Thus, several methods of constructing a membership function as applied to decision-making problems within the framework of fuzzy management of security information and events in CPSs are considered. These methods do not have great mathematical and computational complexity, but they allow to take into account the uncertainty (fuzziness) of the observed and controllable security parameters, which makes it possible to increase the reliability of security information and event management of modern CPSs.

Practical application of the proposed methods for constructing the membership function in fuzzy control problems is possible both within the framework of research work and in the systems of automated control of information security for complex information-telecommunication and cyber-physical systems. The direction of further research can be the development of methods that take into account not only the fuzzy but also the contradictory (incomplete) nature of the initial data characterizing the controlled parameters of systems of this class.

Acknowledgements This research is being supported by the grant of RSF #21-71-20078 in SPC RAS.

References

1. Miller, D.R., Harris, S., Vandyke, S.: Security Information and Event Management (SIEM) Implementation. McGrawHill, New York (2011)
2. Kotenko I., Parashchuk I.: Determining the parameters of the mathematical model of the process of searching for harmful information. Cyber-physical systems: industry 4.0 challenges. In: Kravets et al. A.G., (eds.), Studies in Systems, Decision and Control, vol. 260. Springer Nature Switzerland AG, Cham (2020)
3. Maimbo C.: Exploring the Applicability of SIEM Technology in IT Security: Masters thesis. Auckland, Auckland University of Technology (2014)
4. Takagi, T., Sugeno, M.: Fuzzy identification of systems and its application to modelling and control. IEEE Trans. Syst. Man Cybern. **15**, 116–132 (1985)
5. Carlsson C., Fedrizzi M., Fuller R. (2004) Fuzzy Logic in Management, vol. 2004, p. 288. Springer, Boston (1985)

6. Buckley J.J., Eslami E.: An Introduction to Fuzzy Logic and Fuzzy Sets, vol. 2002, p. 285. Springer, Berlin (2002)
7. De Barros, L.C., Bassanezi, R.C., Lodwick, W.A.: A First Course in Fuzzy Logic, Fuzzy Dynamical Systems, and Biomathematics. Theory and Applications, vol. 2017, 304. Springer, Berlin (2017)
8. Ramya, K., Teekaraman, Y., Ramesh Kumar, K.A.: Fuzzy-based energy management system with decision tree algorithm for power security system. Int. J. Comput. Intell. Syst. **12**(2), 1173–1178 (2019)
9. Gaikwad, D., Jagtap, S., Thakare, K., Budhawant, V.: Anomaly based intrusion detection system using artificial neural network and fuzzy clustering. Int. J. Eng. Sci. **1**, 1–6 (2012)
10. Hooda, D.S., Raich, V.: Fuzzy Logic Models and Fuzzy Control. An Introduction, p. 409. Oxford, Alpha Science International Ltd (2017)
11. Zhang, W.-R.: The road from fuzzy sets to definable causality and bipolar quantum intelligence - to the memory of Lotfi A. Zadeh . J. Intell. Fuzzy Syst. **36**(4), 3019–3032 (2019)
12. Beliakov, G., Pradera, A., Calvo, T.: Aggregation Functions: A Guide for Practitioners. Studies in Fuzziness and Soft Computing. Springer, Berlin GmbH **2007**, 39–122 (2007)
13. Xu, Z., Yager, R.R.: Some geometric aggregation operators based on intuitionistic fuzzy sets. Int. J. Gener. Syst. **35**, 417–433 (2006)
14. Yager, R.R.: Properties and applications of Pythagorean fuzzy sets. Imprecision and Uncertainty in Information Representation and Processing. Springer Nature Switzerland AG, Cham **2015**, 119–136 (2015)
15. Kotenko, I.V., Parashchuk, I.B., Omar T.K.: Neuro-fuzzy models in tasks of intelligent data processing for detection and counteraction of inappropriate, dubious and harmful information. II International Scientific and Practical Conference on the Fuzzy Technologies in the Industry (FTI 2018), Ulyanovsk, 23–25 October 2018. CEUR Workshop Proceedings (CEUR-WS), vol. 2258, pp. 116–125 (2018)
16. Parashchuk I.B., Doynikova E.V.: The architecture of subsystem for eliminating an uncertainty in assessment of information objects semantic content based on the methods of incomplete, inconsistent and fuzzy knowledge processing. In: Kotenko, I., et al. (eds.), The XIII Science Conference of Intelligent Distributed Computing (IDC-2019). Studies in Computational Intelligence, vol. 868 (SCI 868), pp. 294–301. Springer Nature Switzerland AG, Cham (2020)
17. Singpurwalla, N.D., Booker, J.M.: Membership functions and probability measures of fuzzy sets. J. Am. Stat. Assoc. **99**(467), 867–877 (2004)
18. Mingtian, F., Zuping, Z., Chengmin, W.: Optimization of annual generator maintenance scheduling. Selection of fuzzy membership function. In: Mathematical Models and Algorithms for Power System Optimization. Modeling Technology for Practical Engineering Problems, pp. 49–80. Academic, New York (2019)
19. Li-Hua, F., Gao-Yuan, L.: Analysis on fuzzy risk of landfall typhoon in Zhejiang province of China. Math. Comput. Simul. **79**(11), 3258–3266 (2009)
20. Qiang, Z., Jianzhong, Z., Chao, Z., Jun, G., Weiping, D., Mengqi, Y., Li L.: Fuzzy risk analysis of flood disasters based on diffused-interior-outer-set model. Expert Syst. Appl. **39**(6), 6213–6220 (2012)
21. Bojadziev, G., Bojadziev, M.: Fuzzy Logic for Business, Finance, and Management, 2nd edn., p. 252. World Scientific Publishing Co. Pte. Ltd., Singapore (2007) (2007)
22. Chen, G., Trung Tat, P.: Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems, p. 328. CRC Press LLC, Boca Raton (2008)
23. Shahbazova, S.N., Sugeno, M., Kacprzyk, J.: Recent Developments in Fuzzy Logic and Fuzzy Sets: Dedicated to Lotfi A. Zadeh., 1st edn., p. 220. Springer Nature Switzerland AG, Cham (2020)

24. Parashchuk, I.B., Bobrik, I.P.: Fuzzy Sets in Problems of Analysis of Communication Networks, p. 80. St. Petersburg, VUS (2001)
25. Kotenko, I., Parashchuk, I.: Decomposition and formulation of system of features of harmful information based on fuzzy cxsrelationships. In: The 2019 International Russian Automation Conference (RusAutoCon). IEEE Xplore Digital Library: Browse Conferences. 2019, vol. 8867588, pp. 1–5 (2019)