Using fuzzy logic system for making decisions about information security in grid infrastructure

Rodin Y.S., Sinitsyn I.P.

Institute of Software Systems NAS Ukraine

yevheniy.s.rodin@gmail.com, sec_kiev@ukr.net

Abstract. *In purpose of more objective formalization of peer review, reduction of the impact of subjective methods of assessment of risks, increasing of number of the impacts on information risks, in order to model the decision-making mechanism for information security the fuzzy logic system (FLS) has been proposed to use.*

Keywords

Fuzzy logic, information security, risk management, grid.

1 Introduction

Information systems develop rapidly, they turn to distributed systems with plenty of objects, subjects, with variety of information flows. The growing set of factors that affect information security, new processes, states and behaviors in systems and beyond its borders is the consequence of complication of information systems. Therefore the modeling becomes particularly relevant in creating a reliable, flexible protection system.

One of the main purposes of modeling in information security (IS) – is a building a model that takes into account the most influential factors and allows to calculate the likelihood of vulnerability and threat, to calculate the time of the threat and potential damages, to determine the efficiency of protection and degree of protection of the system . Modeling and receipt of the indicators mentioned above will permit to make decisions about IS system and manage information security risks.

2 Related works

A key model that used in the management of information security risks (MISR) is a process model that is reflected in all standard approaches to MISR and is the basis of the ISO / IEC 27005 and BS 7799-3. Process model gives a list, sequence, reveals the essence planning, implementation, test, performance, that required to manage IS risks.

The basis for determining the level of risk in almost all methods is likelihood of occurrence of event that affects the probability of the threat. The determination of likelihood is performed by an expert method or statistics of previous periods on the same events is taken as a base.

Does this method correspond to reality, is it accurate enough? Firstly, it is necessary to propose amendment to the error of experts, and secondly, the statistics of previous periods does not match reality, especially in cases of rapid changes in hardware and software (vulnerability of which is unknown), and thirdly there are more factors influencing the determination of risk than probability of threat and amount of loss.

Nowadays there are works of definitions of information risk, where fuzzy logic (L. Zadeh) is used [1,2]. In these works there are limited influential factors (linguistic variables) used for building rule base, for instance probabilities and losses [3,4,7]. There are works trying to evaluate level of information damage using following linguistic variables confidentiality, integrity and availability [5].

The ideas which presented in this work consist in combining methods of modeling the ontologies, constructing event trees to expand the knowledge base and construct fuzzy rules and membership functions, that as a result will affect comprehensive risk analysis by using FLS.

3 The adaptation of process approach risk management information security of grid infrastructure to fuzzy logic

3.1 Stages of the construction of fuzzy model

The main stages of the construction of fuzzy model are [4]:

- description of entities of environment and defining them in terms of fuzzy logic, formalization of variables
- construction of membership function
- formation of fuzzy knowledge base, forming fuzzy rules
- fuzzification: interpretation of precise input variables as fuzzy intervals
- calculation of fuzzy implication
- approximation of model
- defuzzification: transfer results of fuzzy inference in clear definitions

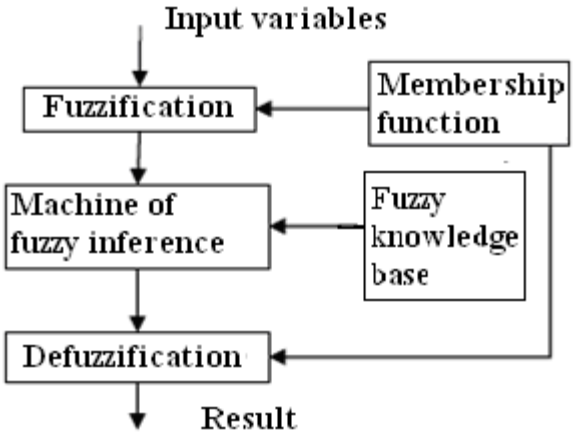

Fig.1 Stages of the construction of fuzzy model

In works about determination of IS risks three factors are defined with the help of FLS. They are risk, the probability of an emergency situation, the level of damages. These factors are converted into linguistic variables to create fuzzy rules, where the probability of the threat and the level of losses are input variables, and the level of risk is the output variable.

Among the membership functions the most popular function is triangular, which is constructed by direct method by using three main terms, α - min, m - modal value, β - max:

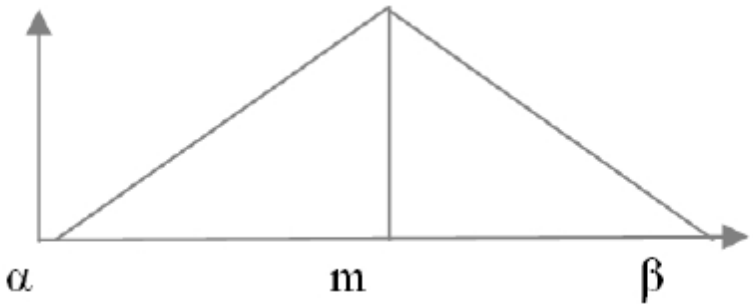

Fig.2 Graphical representation of triangular membership function

The most popular method of defuzzification is the method of choice of precise definition that corresponds to the maximum of membership function, or center of gravity method.

3.2 Formation of the fuzzy knowledge base in IS for grid distributed systems

For forming fuzzy knowledge base by means of processing methods following is proposed to be done:

- classification and a list of resources,
    - defined list of qualitative and numerical (including composite) evaluation criteria of resources,
- classification and a set of vulnerabilities inherent to grid-environment,
    - defined list of qualitative and numerical (including composite) evaluation criteria of vulnerabilities,
- classification and a list of risks,
    - defined list of qualitative and numerical (including composite) evaluation criteria of risks,
- classification and a set of tools and safety measures,
    - defined list of qualitative and numerical (including composite) evaluation criteria of tools and safety measures.

Based on received classifiers in terms it is proposed to convert influential factors in terms of FLS. Those factors are to influence MRIS in grid- infrastructure.

β- the magnitude of risk - linguistic variable

X – universal set - the value of losses in monetary terms,

T - Terms (values of linguistic variable), for example: high risk, medium, small and derived from main terms,

α - fuzzy variable - <name of fuzzy variable - low risk, the domain of definition - losses in monetary terms, fuzzy set to a small risk>.

Example of fuzzy set representing the small risk:

S={x | xєX & M(x)>0}, X –damage set, x – loss meaning in money, describing the fuzzy variable "low risk», M (x) –x membership degree of belonging to the fuzzy definition of "low risk".

The level of allocated (reserved) budget per year for restoration (coating) from the possible loss from of information security incidents can be compared with the value of losses to determine the boundary values of variable fuzzy linguistic variable " magnitude at risk"

Linguistic variables (βi) that affect the magnitude of risk:

β1 - staff skill level, X – percentage of employees with experience more than 5 years,

β2 –level of probability of threat, X – probability (or – number of incidents over the past 5 years) – may consist of probabilities of multiple events,

β3 – The level of probability of the worst-case scenario likelihood (або – number of incidents over the past 5 years) – may consist of likelihoods of multiple events,

β4 – The level of countermeasures cost, X –cost,

β5 – The level of resource criticality, X – possible time of system work without resource,

β6 – The level of reputation loss, availability, confidentiality, integrity,

β7 –duration of treat, X – time scale,

β8 – The level of the allocated budget , X – cost scale.

As input it is proposed to create interaction rules of βi values for each threat.

As output it is proposed to take decision to select scenario action on the threat.

Construction of fuzzy rules is proposed to define with hierarchical fuzzy knowledge base. This base can be constructed by methods of ontologies of entities and information security vulnerabilities of event trees.

For forming membership function it is proposed to use indirect methods to minimize the impact of subjective expert assessments.

4 Conclusion

It is proposed to use processing approach, ontologies and construction of event trees for formation of hierarchical knowledge base. It is proposed to enter additional linguistic variables that influence decisions on information security.

In further work it's necessary to define carefully the membership function of the fuzzy input and output.

References

1. L.A. Zadeh. The concept of linguistic variable and its application to approximate reasoning. *Information sciences*, 8: 199-249, 1975.
2. К Г.Малышев ЛС.Берштейн А. В. Боженюк. Нечеткие модели для экспертных систем в САПР. / Н.Г. Малышев, Л.С. Берштейн, А.В. Боженюк. — М.: Энергоатомиздат, 136с., 1991.
3. Родина Ю. В. Оценка риска нарушения информационной безопасности по модели нечёткой логики с корректировкой параметров её терм-множеств. Управление экономическими системами, 6: 12с., 2011.
4. Кущ С.М., Шутовський В.О. Використання експертних та нечіткологічних систем для оцінки ризиків інформаційної безпеки інформаційно- телекомунікаційних систем. *Вісник Національного технічного університету України "КПІ" Серія – Радіотехніка. Радіоапаратобудування*, №50: 114-120, 2012.
5. Eric Afful-Dadzie1. Arnošt Veselý. User Perception of Security on Social Networking Sites Using Fuzzy Logic. *British Journal of Applied Science & Technology* 3(4): 714-734, 2013.
6. Родін Є.С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки. *Математичні машини і системи*, 4: 142-148, 2012.
7. Ажмухамедов И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования. Монография:344, 2012.