Міжнародна наукова конференція

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ ТА ПРОБЛЕМИ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

ISDMCI'2019

Збірка наукових праць

Аналіз та моделювання складних систем і процесів
Теоретичні і прикладні аспекти систем прийняття рішень
Обчислювальний інтелект та індуктивне моделювання

Херсон
ФОП Вишемирський В.С.
2019

УДК 004.89
І 73

ORGANIZERS

Black Sea Scientific Research Society, Ukraine

Kherson National Technical University, Ukraine

IT Step University, Ukraine

Jan Evangelista Purkyne University in Usti and Labem, Czech

Lublin University of Technology, Poland

Taras Shevchenko National University, Ukraine

V.M.Glushkov Institute of Cybernetics NASU Ukraine

International Centre for Information Technologies and Systems of the National Academy of Sciences of Ukraine, Ukraine

INFORMATION PARTNERS

2020 IEEE Second International Conference
on Data Stream Mining & Processing

It Beans: student community

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ І ПРОБЛЕМИ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

ISDMCI'2019

Міжнародна наукова конференція

І 73 Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту: матеріали міжнар. наук. конф., с. Залізний Порт, 21-25 травня 2019 р. – Херсон: Видавництво ФОП Вишемирський В. С., 2019. – 240 с.

ISBN 978-617-7783-02-1 (*електронне видання*)

У збірнику представлені матеріали наукової конференції «Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту», яка відбулася у с. Залізний Порт 21-25 травня 2019 р. та була присвячена актуальним питанням сучасних методів прийняття рішень та інформаційних технологій.

Матеріали збірки розраховані на викладачів та студентів вищих навчальних закладів, фахівців науково-дослідних установ та підприємств

УДК 004.89

ISBN 978-617-7783-02-1 (*електронне видання*)

11. И.Г. Перова Адаптивная обработка данных медико-биологических исследований методами вычислительного интеллекта // Восточно-европейский журнал передовых технологий. – Х.: 2014. – №1(67), с. 24-28.
12. Perova, Ye. Bodyanskiy Adaptive fuzzy clustering based on Manhattan metrics in medical and biological applications // Вісник національного університету "Львівська політехніка" №826, 2015, p. 8-12.
13. Perova, I., Bodyanskiy, Y., Sachenko, A., Karpinski, M., Rudyk, P. Fuzzy clustering of biomedical datasets using BSB-neuro-fuzzy-model // CEUR Workshop Proceedings, Lviv, 2018, pp. 21-28.

NORMALIZED METHOD FOR THREATS ASSESSING FOR DISTRIBUTED WIRELESS SYSTEMS

Buriachok V.L.[1], Sokolov V.Yu.[2], Skladannyi P.M.[3]

Borys Grinchenko Kyiv University, Kyiv, Ukraine
[1]ORCID: 0000-0002-4055-1494, v.buriachok@kubg.edu.ua
[2]ORCID: 0000-0002-9349-7946, v.sokolov@kubg.edu.ua
[3]ORCID: 0000-0002-7775-6039, p.skladannyi@kubg.edu.ua

The subjective process of obtaining the probability of a threat can be divided into three stages:

– preparatory (the object of research is formed: the set of events and the initial analysis of the properties of this set; one is selected for methods of obtaining subjective probability; the preparation of an expert or a group of experts);

– obtaining grades (using the chosen method; obtaining results in a numerical form, possibly contradictory);

– analysis of the obtained assessments (research results of the survey; clarification of the answers of experts).

Sometimes the third stage is not carried out if the method itself uses axioms of probable distribution, which in itself is close to experts' estimates. Conversely, this stage becomes especially important if results are obtained from a group of experts.

It is also possible to separate two approaches to multi criteria assessment of the efficiency of wireless networks:

– associated with bringing the set of individual performance indicators to a single integral indicator;

– uses methods of the theory of multi-choice choice and decision-making (with a significant number of individual performance indicators, approximately equally important).

The proposed normalized method for assessing the degree of security assurance operates with at least three characteristics, which allows for a comparative analysis of heterogeneous information systems.

The degree of security provides a rough estimate of the effectiveness of the information security system. The method operates with the subjective coefficients of weight i^{th} characteristic W_i and the ball values of each characteristic G_i, which is determined by expert's estimates. The formula for the degree of security is as follows:

$$S = \frac{1}{N}\sum_{i=1}^{N} W_i \cdot G_i \tag{1}$$

where N—amount of the characteristics.

The method has two drawbacks: it is impossible to compare systems with different sets of characteristics and it does not take into account the dependence of the weighting factor and the value of the characteristic of the characteristic itself [1,2]. The author of the paper proposes to use normalized characteristic S^* to assess the degree of the system security, and at the same time, to consider the subjective factors of the importance of the i^{th} characteristic and the ball value of each characteristic, as a function of the characteristics:

$$\begin{cases} W_i = f_W(x_i), \\ G_i = f_G(x_i) \end{cases} \tag{2}$$

where f_W and f_G—function of the characteristic x_i.

The general formula for monotonous f_W and uncertain function f_G is as follow:

$$S^* = \frac{1}{N}\sum_{i=1}^{N} W^*(x_i) \cdot G^*(x_i) \tag{3}$$

where $W^*(x_i)$—normalized weighting factor of subjective estimation from x_i:

$$W^*(x_i) = \left| \frac{f_W(x_i)}{\max\left[f_W(x_i)\right]} \right| \tag{4}$$

and $G^*(x_i)$—normalized score value of a function:

$$G^*(x_i) = \left| \frac{G_i^{\Sigma}}{G_{i\max}^{\Sigma}} \right| \tag{5}$$

Intermediate values of which are defined as integral characteristics:

$$\begin{cases} G_i^{\Sigma} = \int\limits_{x_i^{\text{begin}}}^{x_i^{\text{end}}} f_G(x)dx, \\ G_{i\max}^{\Sigma} = \int\limits_{x_i^{\min}}^{x_i^{\max}} f_G(x)dx \end{cases} \tag{6}$$

where x_i^{begin} and x_i^{end}—the beginning and the end of the range of values for a given characteristic that exists and is continuous in the range from $x_i^{\min}$ to $x_i^{\max}$.

In the given case the normalized level of safety of the system will always be $S^* \leq 1$. S^*—“absolutely” protected system, when all the existing characteristics x_i are considered. In the general case, the proposed modification of the method allows to obtain a normalized level of security for any system with a number of characteristics (but not less than 3), and to conduct a comparative analysis of information security in systems with a different set of characteristics.

Because the method operates with the results, obtained through expert evaluation, before the data processing begins, it is necessary to assess the adequacy of the expert group. To assess the adequacy it’s needed to determine the coefficient of concordance, which involves the elements of functional-cost analysis.

Let’s suppose we have N essential characteristics that are included in the X set of all characteristics of the system $[x_1,x_2\ldots x_N]$ belong to the set X.

We determine experimentally or analytically the intervals of values for all characteristics (minimum and maximum values), as well as the average value (which does not necessarily coincide with the arithmetic mean and maximum values). In the found intervals, experts determine the point values of each characteristic G_i:

$$\begin{cases} G_1 = f_G(x)\big|_{x=\overline{x_1^{\min},x_1^{\text{av}},x_1^{\max}}}, \\ G_2 = f_G(x)\big|_{x=\overline{x_2^{\min},x_2^{\text{av}},x_2^{\max}}}, \\ \quad\ldots \\ G_N = f_G(x)\big|_{x=\overline{x_N^{\min},x_N^{\text{av}},x_N^{\max}}}. \end{cases} \tag{7}$$

Based on the obtained data, for the sake of clarity, the charts (2), used by experts to determine the following characteristics, are constructed [3].

The results of modelling are implemented in the educational process of Ukrainian and foreign institutions of higher education (Blekinge Institute of Technology, State University of Telecommunications, Borys Grinchenko Kyiv University, Lviv Polytechnic National University and Kharkiv National University of Radio Electronics), including two virtual platforms “Cyber Range” for the development of security mechanisms. Thus, the proposed method allows to ensure the reliability and functional safety of the wireless infrastructure, to obtain an effective wireless network and to provide a solution to the problem of “last mile” for subscribers with difficult location. The existing models and methods for assessing security and risks, with their drawbacks were considered in the paper. The proposed modifications are intended to improve existing methods and include more precise approximation (for expected damage to the vulnerability) and generalization of the function (for the degree of security). In addition, it is proposed to use elements of functional-cost analysis to verify the reliability of expert evaluation.

REFERENCES

1. 1. Domarev VV (2001) Security information technology. Methodology for creating security systems. Kyiv, p 688 [publication in Russian]
2. 2. Chipiga AF, Peleshenko VS (2004) Evaluation of the effectiveness of the protection of automated systems from unauthorized access. Bull of North Cauc State Tech Univ, Ser “Phys-Chem” 1(8):40 [publication in Russian]
3. 3. Sokolov VY (2010) Quantitative indicators for assessing security and security risks in distributed systems. Inf Prot 3(48):19–34. DOI: 10.18372/2410-7840.12.1957 [publication in Ukrainian]