Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2020

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2020

UDC 004.01/08

Editorial board:

Black Sea Science 2020: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2020. – 365 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2020» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Odessa National Academy of Food Technologies, 2020.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Serhiy Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies

Members of the jury:

Francisco Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Gerard H. Degla – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics of Odessa National Academy of Food Technologies

Also there were considered the process of path-planning, constructing a curvilinear trajectory, describing the current location of the robot and finding the necessary angle and distance for robot's moving to the next waypoint.

In the course of the work, it was found out that machine learning is a topical subject in the modern world and is a unit of artificial intelligence. Classification and regression were reviewed as the main tasks of supervised learning. There were discussed the possibilities of using in various spheres of human life and given examples of applications in robotics.

The application of machine learning is a topical issue for the modern world and has a great potential for further development. The use of machine learning in robotics can simplify human performance, do it faster and more efficiently. Some companies have already involved in machine learning, such as Google Labs developing a manipulator that can be used for sorting trash based on classification. The main problem now is to transfer this technology to the real world because the robot may encounter objects and tasks that are unknown to it.

VI. References

1. Кинематика: прямая и обратная задачи – URL: http://robocraft.ru/blog/mechanics/756.html
2. Описание движения мобильного робота – URL: http://robotosha.ru/robotics/robot-motion.html
3. Степени свободы (механика– URL: https://ru.wikipedia.org/wiki/Степени_свободы_(механика)
4. Машинное обучение_____– URL: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение
5. Машинное обучение для людей – URL: https://eldf.ru/machine-learning-base-article
6. Гид: алгоритмы машинного обучения и их типы – URL: https://www.sas.com/ru_ua/insights/articles/analytics/machine-learning-algorithms-guide.html#/
7. Роботы-манипуляторы и «умные» руки: над чем работает Google Robotics – URL: https://vc.ru/future/63826-roboty-manipulyatory-i-umnye-ruki-nad-chem-rabotaet-google-robotics

THE ALGORITHM OF INFORMATION SECURITY RISK ASSESSMENT BASED ON FUZZY-MULTIPLE APPROACH

Author: Nataliia Romashchenko
Supervisor: Olexander Shmatko
National Technical University «Kharkiv Polytechnic Institute» (Ukraine)

Abstract*.The* ***subject*** *of the study is the process of assessing the level of information security risk that is being implemented with the help of the fuzzy logic apparatus. The* ***purpose*** *of this work is to develop a methodology for assessing the degree of information security risk, which would avoid the uncertainty factor, that occurs when some parts of*

*information about the analyzed automated information system are absent. The methodology is based on the use of fuzzy logic and fuzzy sets. Which implies the introduction of the term sets for each of the system characteristics and the linguistic assessment of the indicators. The **tasks** to be solved are to analyze existing information security risk assessment methodologies for identifying their strengths and weaknesses. On the basis of the conducted analysis, a new method for assessing the risk of automated information systems information security is proposed. The following **results** were obtained: the advantages and disadvantages of qualitative and quantitative methodologies for assessing the risk degree of automated systems information security were identified; the main stages of the proposed methodology were described. **Conclusion**: The methodology presented in the article provides an opportunity to translate the obtained results of risk assessment from a mathematical language into a linguistic form that is more comprehensible to the decision-maker. This increases the effectiveness of the management of automated information systems protection mechanisms.*

Keywords: *information security, risk assessment, information security risk assessment methodology, fuzzy sets.*

Introduction

The revolutionary development of information technology over the last decade has led to an increase in the number of threat types and their transformation. The modern world has confidently entered the era of high technology. Automated information systems (AIS) are now gaining popularity in solving the problems of providing information base for various services that deal with technical, economic and other issues. In the process of operation, they can be vulnerable to various threats, which are also modified and have become hybrid. Currently, they combine influences on information security (IS), cyber security (CySec) and security of information (SI). The main target of hybrid attacks is the country's economic sector. With the increase in the amount of data processed, the value of information for business is increasing. In this regard, the task of information security (InfoSec) is becoming increasingly relevant.

There is a need for hybrid technologies to counteract risks that play a significant role in business processes. That is why during the design and development of reliable AIS, it is necessary to provide a set of measures aimed at ensuring their protection against intentional or accidental influences, which can lead to disruption of the system. Such failures in AIS work entail serious losses in the form of assets or material resources, deterioration of the image of the owner or developer of AIS.

Information security threats to automated information systems that directly affect the system include internal and external threats to staff and its customers. Both the former and the latter in their targeting and nature of influence on the activity of certain subjects and objects can be economic, physical and intellectual [1], [2].

Information security is part of managing the information system as a whole. One of the most important components of the InfoSec management system is risk assessment, which is designed to determine the effectiveness of the security mechanisms based on specific metrics. The challenge remains to refine existing methods of assessing IS risk in view of the emergence of new types of threats. Therefore, the purpose of the work is to increase the level of information security of automated information systems by introducing

an automated methodology for assessing information security risks based on the use of fuzzy sets.

Analytical review of literature

Research priority areas in the field of information security are:

— development of security threats models to information and telecommunication systems (ITS) and ways of their implementation;

— determining the criteria of systems vulnerability and resilience to destructive effects;

— development of monitoring methods and means for revealing the facts of unauthorized information influences;

— development of methodology and methodological apparatus for assessing damage from information security threats;

— improvement of existing methodologies for risk assessment and its further management [3].

To ensure information security it is equally important to develop methods and tools for information security of information and telecommunication systems, including automated security management systems, methods and means of key distribution and protection of information and information resources from unauthorized access and destructive information impact, anti-virus technologies, methods and means of control of protection conditions against unauthorized access of modern and perspective technical means and solution of the problem of guaranteed destruction of residual information on magnetic media, research and development of methods of designing secure systems using unreliable (from the point of information security view) elements, including the problem of their testing.

Urgent tasks stem from the rapid development of information and telecommunication systems, which today are transformed into distributed systems of multiple objects, entities, with various information flows and connections. The consequence of the complication of information systems is the growing number of factors affecting information security, the emergence of new processes, states and variants of behavior in systems and beyond. Therefore, when creating reliable, flexible systems of protection modeling is of special relevance. One of the main goals of information security modeling is to build a model that takes into account the largest number of influential factors and allows to calculate the probability of vulnerability and threat realization, to calculate the time of realization of the threat and possible losses, to determine the effectiveness of implementation of security measures and the level of protection. Modeling and deriving the above metrics will allow you to make decisions about your InfoSec system, that is, manage information security risks.

The basis of AIS information security management is risk analysis. In fact, the risk is an integral assessment of how effectively existing defenses are able to withstand information attacks.

There are usually two main groups of methods for calculating security risks. The first group allows you to set the level of risk by assessing the degree of compliance with a specific set of information security requirements. The second group of information security risk assessment techniques is based on determining the likelihood of attacks and their levels of damage. The value of the damage is determined by the owner of the

information resource, and the probability of an attack is calculated by a team of experts who conduct the audit procedure.

In today's scientific community, there is a large number of researchers whose work focuses on assessing information security risk for systems. For example, in [4] the existing InfoSec risk analysis is classified, the sequences of risk analysis processes are described, a comparison of software tools for risk management of InfoSec is presented. Another example of research in this subject area is the work [5], [6], which describes methods of risk assessment and management.

Article [7] proposes mathematical formulation of risk using the basic concepts of InfoSec of such risk management methodologies as Mehari, Ebios, CRAMM and SP 800-30 (NIST).

The basics for risk assessment, in particular in the context of the risk assessment of access control systems that make authorization decisions, are set out in [8].

In [9], approaches and software solutions for information risk assessment and control are considered as a fundamental organizational stage in the construction of information security systems for computerized systems.

In [10], an advanced methodology for estimating information risk in an automated system was proposed and analyzed. The necessary normative legal documents of information security are covered. The work of a prototype of an expert system is considered, which allows to estimate the level of information risk for a certain automated system and to determine the necessity of application of additional information security measures [11].

The work [12] analyzes the process of work of the most common models of information security risk assessment in information and telecommunication systems. The basic approaches to the assessment of information security risks are revealed.

An analysis of information security threats and a detailed description of intentional sources, classification and causes of their occurrence are given in [13].

Object, subject matter and methods of research

According to the purpose of the work, the object of the work is the process of assessment information security risk level for automated information systems. The subject is algorithmic support for information security risk level assessment of automated information systems.

After analyzing the existing scientific literature from the specified subject area, two main groups of methodology for assessing information security risks are possible to determine: quantitative and qualitative.

Quantitative methods use measurable, objective data to determine the value of assets, likelihood of loss and associated risks. The goal is to calculate the numerical values for each of the components collected during the risk assessment and analysis of costs and benefits.

Qualitative methods use a relative risk or asset value based on rating or categorization, such as low, medium, high, not important, important, very important, on a scale from 1 to 10. A qualitative model evaluates the actions and probabilities of identified risks at a rapid rate and in a cost-effective way. Risk sets are written and analyzed in a qualitative risk assessment, and can serve as a basis for a targeted quantitative assessment.

Quantitative and qualitative information security risk assessment methods have both advantages and disadvantages

Accordingly, the combination of quantitative and qualitative methods represents a mixed set of advantages and disadvantages of the above mentioned methods.

Table 1 – Advantages and disadvantages of qualitative and quantitative risk assessment methods of InfoSec

+/–	Quantitative	Qualitative
Advantages	- risks are the financial consequences priority; - assets are the financial values priority; - obtaining simplified risk management results and investment returns into providing security; - results can be expressed in specific management terminology (for example, monetary value and probability is expressed as a certain percentage); - Accuracy tends to increase over time as the business constantly records data.	- Provides clarity and understanding of risk classification; - the opportunity to reach consensus; - there is no need to determine the financial value of assets; - it is easier to involve people who are not experts in the field of computer security.
Disadvantages	- Importance influence attributed to risks on the basis of judgmental opinions of participants; - the process for achieving reliable results and consensus takes a lot of time; - calculation might be complex and time-consuming; - the results are presented only in monetary terms and they are difficult to interpret for "non-techies"; - the process requires special knowledge, so it is difficult to train staff.	- insufficient distinction between among significant risks; - it is difficult to justify investments in control of implementation, because there are no grounds for the analysis of costs and benefits; - The results depend on the quality of the created risk management team

Security risks of information systems are very closely related to uncertainty. Two cases of uncertainty can be determined: identification of the current and future state of the systems.

When solving tasks related to security risk assessment, the question about the qualitative interpretation of certain levels of parameters often arises. The linguistic assessment of the security level is clearer and best describes the state of IT infrastructure security, which in turn encourages the manager to take one or another decision.

In order to fulfill the linguistic assessment, two things are required:

First, you need to define a linguistic scale for evaluation. Most often pentascale is used (five-level classifier) "Very low (VL) – Low (L) – Average (A) – High (H) – Very high (VH)."

Secondly, it is necessary to collect all available information to define linguistic assessment: quantitative data collected in a group of similar objects of observation.

For example, for a qualitative assessment of the level of information security, it is necessary to collect statistical information on similar information systems for a relatively short period of monitoring. This is necessary to maintain the condition of statistical homogeneity. At the same time, it is necessary to take into account the laws that are inherent to the objects of information security.

It should be noted that there are no general universal rules for accurate and rapid assessment of AIS information security. A set of problems may also arise with the collection of initial data for linguistic analysis.

There is a question connected to the additional data analysis, which is related to different time segments of observations. There may be a question about replacing the

missing data in one-time period with the data from another similar one, and the parameters of this law will be given according to special rules in order to satisfy the necessary authenticity of the identification of the monitoring law.

The presence of quasistatistics makes it possible to make qualitative conclusions about the behavior of a particular parameter of the investigated IS, makes it possible to conduct a linguistic analysis of input data.

Basic steps of the linguistic classification:

1. The studies of the source data set and its verification as a quasi-statistic are conducted. There is evidence that some data distribution law is hidden in these data, for example, the "gray" Pospelov scale.

2. Next, define the main nodes. In the absence of expert evaluation, nodal points can be determined by the simple rule: node point – left end of media interval, nodal point – right end of media interval, middle point – corresponds to the maximum histogram or median histogram.

3. The interval between the two nodal points standing next is divided into three zones, the middle one is the zone of expert uncertainty in the classification. Thus, the primary linguistic interpretation of the histogram is complete.

After the classificatory definition it is possible to make a correction of pestascale. To do this, you can modify nodal classification points, bringing them closer together and narrowing the uncertainty zone. You can also replace the nodal point with an absolute confidence interval and try to expand it on both sides of the nodal point. All clarifications must be made on the basis of an agreed expert evaluation.

Work results

The main result of this work is the proposed methodology for the risk assessment of AIS InfoSec, which is based on a fuzzy-multiple approach:

Stage 1. In the first stage, term sets are introduced to describe the basic sets of the IS state and the subset of states, described in the natural language:

The complete set of information security status assessment E of IS is broken down into five subsets of the form:

E_1 – subset of states "extremely unsuccessful state of IS InfoSec";

E_2 – subset of states "unsuccessful state of IS InfoSec";

E_3 – subset of states of "average quality of the IS InfoSec state";

E_4 – subset of states "relatively safe state of IS InfoSec";

E_5 – subset of states "the maximum safe state of the IS InfoSec".

The corresponding set E of a full risk set of IS InfoSec threats G is divided into 5 subsets:

G_1 – subset of "marginal threat risk of InfoSec";

G_2 – subset of "high threat risk to InfoSec";

G_3 – subset of "average threat risk to InfoSec";

G_4 – subset of "low threat risk to InfoSec";

G_5 – subset of " insignificant risk threat to InfoSec".

Assume that G takes the value from zero to one by definition.

For an arbitrary separate indicator of the InfoSec assessment X_i, the complete set of its values of B_i is divided into five subsets:

B_{i1} – subset "very low level of indicator X_i";

B_{i2} – subset of "low level of indicator X_i";
B_{i3} – subset of "average level of indicator X_i";
B_{i4} – subset of "high level of indicator X_i";
B_{i5} – subset of "very high level of indicator X_i".

An additional condition for matching the sets *B*, *E* and *G* of the following form is performed: if all the indicators in the analysis have, according to the classification, the level of the subset B_{ij}, then the state of the InfoSec is qualified as E_j, and the degree of InfoSec threat risk is qualified as G_j. Fulfilment of this condition affects the correct quantitative classification of the levels of indicators and the correct determination of the level of significance of the indicator in the evaluation system.

Stage 2. Construct a set of indicators $X = \{X_i\}$ in the number $N = 4$, which, according to expert-analyst, on the one hand, affect the assessment InfoSec threat risk, and, on the other hand, evaluate the different sides of IS InfoSec.

Stage 3. Summarize to each indicator the level of its significance for the analysis of ri. To estimate this level, you need to position all the values in descending order of magnitude so that the rule is complied with:

$$r_1 \geq r_2 \geq ... \geq r_n \quad (1)$$

If the system of indicators is put in descending order of their significance, then the significance of the *i*-th index should be determined by the Fishburn's rule [15]:

$$r_i = \frac{1}{N} \quad (2)$$

The Fishburn's Rule reflects the fact that nothing is known about the level of significance of the indicators (1). Then the estimate (2) corresponds to the maximum entropy of the existing information uncertainty about the object of the study

If all the indicators are of equal significance, then

$$r_i = \frac{2(N-i+1)}{(N-1)N} \quad (3)$$

Stage 4. Construct a classification of the current value g of the risk factor G as a criterion for dividing this set into a subset (Table 2):

Table 2 – Value of indicator *g*

Interval *G*	Set names
$0.8 < g < 1$	G_1 – subset of "marginal threat risk to InfoSec";
$0.6 < g < 0.8$	G_2 – subset of "high threat risk to InfoSec";
$0.4 < g < 0.6$	G_3 – subset of "average threat risk to InfoSec";
$0.2 < g < 0.4$	G_4 – subset of "low threat risk to InfoSec";
$0 < g < 0.2$	G_5 – subset of " insignificant risk threat to InfoSec".

Stage 5. Construct a classification of the current values x of the X indicators as a criterion for breaking up the complete set of their values into a subset of type B (Table 3).

Table 3 – Value subset partition

Indicator name	Criteria of subset partition				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	$x_1<b_{11}$	$b_{11}<x_l<b_{12}$	$b_{12}<x_l<b_{13}$	$b_{13}<x_l<b_{14}$	$b_{14}<x_l$
…	…	…	…	…	…
X_i	$x_i<b_{i1}$	$b_{i1}<x_i<b_{i2}$	$b_{i2}<x_i<b_{i3}$	$b_{i3}<x_i<b_{i4}$	$b_{i4}<x_i$
…	…	…	…	…	…
X_N	$x_N<b_{N1}$	$b_{N1}<x_N<b_{N2}$	$b_{N2}<x_N<b_{N3}$	$b_{N3}<x_N<b_{N4}$	$b_{N4}<x_N$

Stage 6. Evaluate the current level of indicators and reduce the results:

Таблиця 4 – Indicator's level evaluation

Indicator name	Current value
Very high (VH)	$X_1>1$
High (H)	$0.1< X_2 <1$
Medium (M)	$0.01< X_3 <0.1$
Low (L)	$0.001< X_4 <0.01$
Very low (VL)	<0.001

Stage 7. Classify the current values of x according to the criterion of Table 3. The result of the classification is Table 5. $\lambda_{ij}=1$, if $b_{i(j-1)}<x_i<b_{ij}$, and $\lambda_{ij}=0$, when the value does not fall into the selected range of classification.

Table 5 – Classification result

Indicator name	The result of classification by subsets				
	B_{i1}	B_{i2}	B_{i3}	B_{i4}	B_{i5}
X_1	λ_{11}	λ_{12}	λ_{13}	λ_{14}	λ_{15}
…	…	…	…	…	…
X_i	λ_{i1}	λ_{i2}	λ_{i3}	λ_{i4}	λ_{i5}
…	…	…	…	…	…
X_N	λ_{N1}	λ_{N2}	λ_{N3}	λ_{N4}	λ_{N5}

Stage 8. Carry out arithmetical steps to assess the degree of bankruptcy risk of *g*:

$$G = \sum_{j=1}^{5} g_j \sum_{i=1}^{N} r_i \lambda_{ij} \quad (4)$$

$$g_j = 0.9 - 0.2(j-1) \quad (5)$$

r_i is defined by formulas (2) and (3).

The contents of formulas (4-5) is as follows: first, we evaluate the significance of a particular subset B in the assessment of state E and in the assessment of the threats risk level G. These index numbers are further involved in the external summation to determine the average value of *g*, where g_j is the average estimate of *g* from the corresponding range of table 2 of the method stage.

Step 9. We classify the obtained value of the degree of risk of InfoSec on the basis of table 2. Thus, the conclusion about the threat risk level of AIS InfoSec takes on a linguistic form.

Conclusions

The relevance of the issues for information security risk assessment of automated information systems is considered in the paper. Existing methods of risk assessment of AIS InfoSec are considered.

After analyzing the literature, the techniques were classified into two principles - those that provide a qualitative risk assessment; those that provide a quantitative risk assessment. The advantages of each type of methods and their disadvantages are revealed. In the course of the analysis, it was found that the most effective assessment is given by mixed types of methodologies that combine the characteristics of both types of assessment.

During the course of the work, a risk assessment technique was developed based on a fuzzy multiple approach that avoids the uncertainty factor during the process of assessing the system security degree and obtains the risk level in a linguistic form. The proposed methodology assesses the risk of a mixed type – combining qualitative and quantitative characteristics.

Reference

1. Judin, O.K., (2011). Information security. Regulatory support. Kyiv: NAU.
2. Lenkov, S. V., Peregudov, D. A., & Horoshko, V. A. (2008). Methods and means of information protection. Kyiv: Arij.75-79 c., 2008.
3. Puzyrenko, O.G., Ivko, S.O. & Lavrut, O.O., (2014). Analysis of the process of information security risk management in providing information and telecommunication systems. Systems of information processing, 8(124):128-134.
4. International Journal of Computer Applications (0975 – 8887) Volume 103 – No.8, October 2014 36 Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk Mohamed Ghazouani ENSEM Casablanca, MAROC S.
5. A Framework for Risk Assessment in Access Control Systems Hemanth Khambhammettua, Sofiene Boularesb, Kamel Adib, Luigi Logrippoba Price Waterhouse

Coopers LLP, NewYork, NY, USA Universit´edu Qu´ebecen Outaouais, Gatineau, Qu´ebec, Canada.

6. Chunarova, A. V., Parhomenko, I. I. & Sashhuk, I. I., (2014). Analysis of approaches and software solutions for the assessment and control of information risks in the computerized. Bulletin of the Engineering Academy of Ukraine, 2:138-142.

7. Buchyk, S. S., (2017). Methodology for assessing information risks in an automated system. Knowledge-based technologies, 3 (35):224.

8. Buchyk, S. S. & Shalaev, V. A., (2017). Analysis of instrumental methods for determining information security risk information and telecommunication systems. Knowledge-based technologies, 3(35):215-225.

9. Puzyrenko, O. G., Ivko, S. O., Lavrut, O. O. & Klymovych, O. K., (2015). Application of information security risk assessment models in information and telecommunication systems. Systems of information processing, 3(128):75-79.

10. Gonchar, S., (2014). Analysis of probability of realization of threats of information protection in automated control systems of technological process. Information protection, 16(1):40-46.

11. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 4th ed. Englewood Cliffs, NJ: Prentice-Hall, 2006.

12. Sarvin, A., Abakulina, L., (2003). Diagnostics and over automation of systems: Written lectures. SPB.: SZTU. – 69 c.

13. D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems," IEEE Security Privacy, vol. 4, no. 2, pp. 40–49, Mar. 2006.

14. Slobodenuk, D., (2013). Banking technologies, information security tools in banking systems. // http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html, 15.01.2020.

15. SS 34.311-95. Information technology. Cryptographic information security. Hash function– K.: SS of Ukraine, 1998.

INTELLIGENT AGENT OF ACCESS MANAGEMENT AND CONTROL SYSTEM

Author: Denys Vysoven
Supervisor: Artem Kovalchuk
National Technical University of Ukraine
«Kyiv Sikorsky Polytechnic Institute» (Ukraine)

Abstract.*This article is devoted to the research and development of an agent for a distributed system of access management and control. It consists of different modules, which allows for addition of new features and improves its security and redundancy capabilities. This system allows for a precise control of movement of authorized and unauthorized personnel.*

Keywords: *distributed systems, multiagent systems, ACS systems, security*