International Journal of Civil Engineering and Technology (IJCIET)
Volume 10, Issue 03, March 2019, pp. 454-463, Article ID: IJCIET_10_03_046
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=10&IType=03
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

DEVELOPMENT OF A MODEL OF CYBER SECURITY MANAGEMENT FOR AUTOMATED SYSTEMS

K. Sauanova
Associate Professor, Almaty University of Power Engineering and Telecommunications, Kazakhstan

S. Sagyndykova
Associate Professor, Almaty University of Power Engineering and Telecommunications, Kazakhstan

V. Buriachok
Professor
Doctor of Technical Sciences, Department of Information and cyber security,
Borys Grinchenko Kyiv University, Kyiv, Ukraine

N. Mazur
PhD in Pedagogical Sciences, Department of Information and cyber security,
Borys Grinchenko Kyiv University, Kyiv, Ukraine

A. Anosov
PhD in Technical Sciences, Associate Professor, Department of Information and cyber Security, Borys Grinchenko Kyiv University, Kyiv, Ukraine

S. Smirnov
PhD
Cyber Security & Software Academic Department
Central Ukrainian National Technical University, Kropivnitskiy, Ukraine

V. Malyukov
Professor
Department of Computer systems and networks, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine

ABSTRACT

A model of a system of managing information security of automated data processing systems of critical application is offered in the article. The model allows to evaluate the level of risk for the information security and provides support of decision-making on the counteraction to the unauthorized access to the information circulating in the information systems.

Key words: information protection, information security, automated data processing systems, information security risk, and decision-making.

Cite this Article: K. Sauanova, S. Sagyndykova, V. Buriachok, N. Mazur, A. Anosov, S. Smirnov and V. Malyukov, Development of a Model of Cyber Security Management for Automated Systems, International Journal of Civil Engineering and Technology, 10(03), 2019, pp. 454-463

http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=10&IType=03

1. INTRODUCTION

Modern technologies of open distributed systems and network integration underlying the functioning of the automated data processing systems of critical application (ADPS CA) and telecommunications networks have a large number of vulnerabilities [1-3]. The intervention in national, regional and municipal ADPS CA in energy sector, industry, transport, communications etc. is a frequently mentioned threat of cyber-attacks of criminals [4-9]. In this regard, the issues of information security (IS) and information protection in ADPS CA have acquired increasing importance in recent years.

During the last decades the concept of IS was identified primarily with the terms – confidentiality, integrity and availability of information. At the same time, the implementation of an information security policy (ISP), for many years was assigned to the technical systems and means of information protection (TSMP). According to the generally accepted approach to the implementation of the ISP, the information procedures (IP) successfully counteract to the predefined cyber threats during the operation of ADPS CA within the known external conditions. Thus, the continuous development of methods and means of information protection (MIP), leads to the evolution of algorithms of implementation of cyber-attacks, and the emergence of new MIP is accompanied by new scenarios of cyber-attacks [10-13].

The flexibility of information security management system (ISMS) within the context of ensuring the confidentiality and availability of information is correlated with the algorithms that differentiate access to information processes (IP) in ADPS CA. The adopted security policy model (SPM) determines the existence of certain vulnerabilities of the IP. It should be noted that any SPM responsible for reliable processing of information, must maintain a global security policy (SP), which determines the required parameters of IP, and can contribute to the local SP, regulating rules of transition of IP between adjacent states of ADPS CA.

In the existing ISMS, decision-making becomes difficult due to the following reasons: to form a complete set of IS threats in advance is not always possible; the degree of criticality of the situation and its forecasting in the dynamics is quite difficult to perform and others. Thus, often incomplete and uncertain initial data on the state of MIP, possible threats, destabilizing effects etc., cause issues associated with IS and cyber defence of ADPS CA.

2. PROBLEM STATEMENT

The aim of the research – approbation of the model of ISMS, assessment providing of criticality of the situation with the information protection in ADPS CA and capable to assess the risks' levels connected with the violation of IS and cyber security.

3. MATERIALS AND RESEARCH METHODS

From the viewpoint of evaluating the effectiveness of provision of IS of ADPS CA, it can be represented as a set of components, each of which ensures the implementation of its function of information security (FIS).

Basic components of ADPS CA are: communication network; informational and document flow subsystems; a set of system services. ADPS CA architecture is characterized by: a unified information and communication system, distributed computing tasks and resources, the variety of ways of hardware and software implementation of the functional subsystems, standardized interfaces, regulated connection to global networks. Each of the functional subsystems consists of a set of typical complexes of automation facilities (CAF), implementing processes and procedures of the same type for processing information in the composition of ADPS CA.

As the basic research methods of ISMS of ADPS CA, the following were used: system analysis; the theory of probabilities; mathematical statistics; fuzzy logic.

Let us describe elements of MIP of ADPS CA as evaluation objects – O_i $(i = 1, 2, ...m)$. It is obvious that each of the elements of MIP ensures implementation of concrete FIS_{ij} ($i = 1, 2, ..., m, \quad j = 1, 2, ..., n_i$) where n_i – number of FIS for MIP components – O_i.

When constructing the model of ISMS, the assumption is made that the interpretation of the concept of IS is wider than the term "security of information technologies" in the automated data processing systems, i.e.

$$FIS = \{FIS_{ij} : i = 1,2,..., m : j = 1,2,..., n\} \cup \left\{FIS_{q+v} : q = \sum_{i=1}^{n} n_i, v = 1,2,..., h\right\} \quad (1)$$

where $q = \sum_{i=1}^{n} n_i$ – summation of FIS for all evaluation objects of O_i.

It can be assumed that the elements of a set of FIS_{ij} may not completely ensure the requirements of IS. For example, this may occur in cases of emergence of new types or classes of cyber threats and vulnerabilities in the ADPS CA, which in its turn leads to increasing of the information risk. Now, as a rule, the level of risk is set that is considered acceptable and does not require the adoption of measures to counteract attempts of unauthorized access to ADPS CA [1, 3, 6, 9, 13].

The following assumptions were taken during the development of the model and the algorithm of ISMS.

1. Actions of the attacking side influence ADPS CA and can lead to the loss of data integrity or partial non-fulfilment of the functions of IS.
2. The impact of the attacking side is probabilistic in nature.

3. The impact of the attacking side can be directed both from the outside the company and ADPS CA and from the inside.
4. Assessment of the attacking side impact's consequences was based on statistical analysis methods.

Previously [4] it was suggested to use a special indicator for quantitative characteristic of the degree of current danger of attack or unauthorized access to the ADPS CA, which can be calculated (measured) at any time – index of current risks (ICR) $C_{ICR} = C_{ICR}(\overline{X})$, where $\overline{X}_{ICR} = (x_{ICR_1},..., x_{ICR_i},..., x_{ICR_{MI}})$ – vector of values of ICR, MI – the number of information threats. It is assumed that $C_{ICR} = (0 \div 1)$.

At the first step of work of the algorithm of ISMS the task of obtaining quantitative values that characterize the implementation of FIS_{ij} of MIP of ADPS CA. For each of the functions of IS (FIS_{ij}) such value is the probability that a certain function of IS – FIS_{ij}, for example, control of integrity of software and information support, will be reliably performed within a certain time interval. At a given time interval τ probability of trouble-free execution of FIS_i based on the theory of reliability can be described by the following equation:

$$P_{FIS_i}(\tau) = e^{-\frac{\tau}{T_{mt_i}}}, \tag{2}$$

where T_{mt_i} – average time interval of trouble-free execution of FIS_i.

If it is needed to perform the assessment of costs Z_i, necessary to ensure trouble-free implementation of FIS_i of MIP of ADPS CA, it is possible to use the following relationship:

$$P_{FIS_i}(\tau) = e^{-\frac{\varphi_i \tau}{Z_i}}, \tag{3}$$

where φ_i – the proportionality factor.

The next step is to obtain a quantitative assessment of the figure of current informational risks arising from incomplete execution of FIS_{ij}.

The basic approaches to the analysis of ADPS CA vulnerabilities, and assessment of their degree of IS, are based on analytical calculations and simulation modelling. However, in MIP based on the fuzzy approach, especially with a large number of variables, it is practically impossible to take into account the synergism that can arise at co-occurrence of certain specific values of the individual variables, and it is impossible to ensure the account of differences in the importance of factors influencing the decision-making.

These circumstances make it expedient to develop a technology that would be more consistent with the model, "a multi-dimensional input - output", and made it possible to take into account not only the value of the factors affecting the original variable, but also to determine the degree of importance of controlled parameters when making a decision, and their interaction in the necessary order. Considering all the above mentioned, in this ISMS block, the decision-making algorithms were used in the conditions of fuzzy input information when determining the dimensions of vulnerability of information resources of ADPS CA.

The following assumptions are made:

1. there is a set of controlled input parameters p_{FIS_i} $(i = 1, 2, ..., M)$, the estimates of which were obtained at the previous step of the algorithm, for example, T_{mt_i} and P_{FIS_i} (P_{FIS_i} – P_{im} – the probability of launch of communication centre service of software and information support of ADPS CA in the next working session);
2. it is necessary to obtain a quantitative estimate of the parameter $C_{ICR} = C_{ICR}(\overline{X})$; at the same time it should be considered that when the character of features is probabilistic (when solving the problem of recognition of cyber threats, cyber attacks and anomalies in ADPS CA – the parameter estimation task is C_{ICR}), i.e. when between the features and the measures to which they may be assigned, there are stochastic connections, it is appropriate to conduct the synthesis of algorithms, the recognition, based on the application of the theory of statistical decisions. In the situation when in ISMS there is a complete initial priori information, these results can be used directly. With incomplete initial information the recognition algorithms can also be based on the results of the theory of statistical decisions. Although in the latter case, these results can be used only by implementing algorithms of adaptive learning or self-learning. The next quantitative measure for the assessment is proposed C_{ICR} :

$$\mathrm{IM}_{\mathrm{MN_j},\sigma_i} = \frac{P(MN_j / \sigma_i)}{P(MN_j)}, \tag{4}$$

where $P(MN_j)$ – the probability that a means (method) is used to prevent the threat to IS MN_j; R_1, R_2– a sign of threat to IS of ADPS CA, for example, a sudden increase in traffic, if there is a system of features $\mathrm{SF_n}$ of IS violation, i.e. value $C_{ICR} \to 1$, it is possible to use the following dependence:

$$IM_{MN_j,SF_n} = \sum_{i=1}^{\theta_j} IM_{MN_j}\sigma_i + \sum_{i=l}^{L} IM_{MN_j}\sigma_i, \tag{5}$$

where $i = 1,..., \theta_j$ – the number of independent features, describing the method MN_j ; $l = 1,..., L$ – the number of groups of independent features.

there is a set of linguistic terms T, characterizing the values of the input (φ_v^i, where $v \in [1, N_i]$, N_i – the number of terms of the parameter p_{FIS_i}) and output (δ_j, $j \in [1, N]$, where N – the number of terms of the parameter C_{ICR}) parameters.

An analytical model of the membership function of the variable φ_i to the fuzzy term T is represented in the following form [4]:

$$\mu^T(\varphi) = \frac{1}{1 + \left(\frac{\varphi - \chi}{\beta}\right)^2} \tag{6}$$

where χ and β – setting options of FIS_{ij}; χ – max value of FIS_{ij}; $\mu^T(\chi)=1$ – (χ – the most pragmatic value of the variable φ_i for the fuzzy term); β –concentration factor – stretching of FIS (FIS_{ij}).

For example, when implementing tests on penetration in ADPS CA [9], a series of N measurements of values of the controlled variables φ_i was conducted, in the result of which the following matrix was obtained:

$$H=\begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1i} & \cdots & \varphi_{1n} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2i} & \cdots & \varphi_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \varphi_{l1} & \varphi_{l2} & \cdots & \varphi_{li} & \cdots & \varphi_{ln} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \varphi_{N1} & \varphi_{N2} & \cdots & \varphi_{Ni} & \cdots & \varphi_{Nn} \end{pmatrix}.$$

The first stage of simulation with fuzzy knowledge base consists of the formation with the expert information of the model of the evaluation object (O_i) by building a knowledge base. The second stage is necessary for setting the fuzzy model by its training on the experimental data. Training of ISMS model of ADPS CA lies in the selection of the parameters of membership functions by minimizing the difference between the experimental and theoretical data.

Assuming that:

$B=\{b_i\}$ – knowledge base, where $i=\overline{1,\Omega}$, $\Omega=|B|$ – number of objects (of evaluation) in the knowledge base, for example, integrity monitoring service – P_{im};

$A=\bigcup_{i=1}^{\Omega} A_i$ – the plurality of all attributes in the knowledge base (where $A_i=\{a_{ij}\}$ – the plurality a_j – of the attribute over a plurality of objects O_i);

$j=\overline{1,m}$ – the general number of attributes O_i – of the object of MIP and ADPS CA.

The solution includes the following stages:

1. Define the plurality $P_{FIS}=\{P_{FIS_i}:i\in[1,M]\}$, which can include all or selective evaluations of performance indicators of FIS_{ij} MIP of ADPS CA, as well as the number of terms and their meanings for each of the monitored input parameters φ_i $\Omega=|B|$.
2. Build a fuzzy knowledge base B as a set of production rules of the kind

$$\Psi:\prod_{i\in[1,M]}\{\varphi_v^i : v\in[1,N_i]\}\rightarrow\{\delta_j : j\in[1,N]\}.$$

From the pre-built fuzzy logic conclusion system, we obtain the membership function for all elements of the set of FIS:

$$\{P_{\varphi_v^i}(\varphi_i):i\in[1,M],v\in[1,N_i]\}$$

and for C_{ICR}: $\{C_{ICR_j}(\delta) : j \in [1, N]\}$

where φ_i and δ – input and output parameters with attributes – *A*.

1. On the base of numerical values of $P_i(\tau)$, characterizing the performance of security functions of MIP of ADPS CA, we obtain estimates of input parameters, $(i \in [1, M])$, corresponding to the current indicators of implementation of FIS_i of MIP.
2. Conduct the fuzzification (comparison of the plurality of values of φ_i its membership function, i.e. translation of values of φ_i in the fuzzy format) of input parameters. Define the values of the membership functions corresponding to the estimates of the 4th step of the algorithm: $\tilde{P}_{\varphi_v^i}$, $v \in [1, N_i]$, $i \in [1, M]$
3. Define degree of truth for each of the production rules (PR) of ISMS of ADPS CA.
4. Construct the resulting membership function of $\hat{C}_{ICR}(\delta)$ for the output parameter taking into account the degrees of truth of all PR of ISMS of ADPS CA.
5. The calculation of probability indicators of IS for each class of IS threats is defined by the following iterative dependency [4]:

$$\mathrm{P}_\tau(C_{ICR}) = \frac{P_{\tau-1}(C_{ICR}) \cdot \left\{ P(MN_j/\chi) \cdot P(MN_j/SF_n) + \frac{\sum_{\chi=1}^{\chi} P(MN_j/\chi)}{\chi} \cdot \left[1 - P(MN_j/SF_n)\right] \right\}}{\sum_{\chi=1}^{\chi} \left\langle P_{\tau-1}(C_{ICR}) \cdot \left\{ P(MN_j/\chi) \cdot P(MN_j/SF_n) + \frac{\sum_{\chi=1}^{\chi} P(MN_j/\chi)}{\chi} \cdot \left[1 - P(MN_j/SF_n)\right] \right\} \right\rangle} \quad (7)$$

where χ – the number of class of threats of IS of ADPS CA, τ – the time of threats detection.

Calculate the resulting value of C_{ICR} of the output parameter as a result of defuzzification of a fuzzy plurality $\hat{C}_{ICR}(\delta)$.

It is assumed that the parameters' ranking is carried out at the design stage of MIP of ADPS CA and is not the subject of this study.

In this article let us consider in more detail the procedure of evaluation of ensuring the integrity of software and information support of ADPS CA.

Flexibility of ADPS CA protection algorithms in the context of ensuring the integrity of information, comes down to the need to keep away the negative impact of integrity monitoring service (IMS) on the efficiency of data arrays processing procedures. The consequence of the absence of such restrictions is the diversion of resources of computer, first of all, of the temporary ones from the direct functional tasks of ADPS CA. At the same time the required parameters of IS are achieved through the stepwise organization of IMS.

To support decision-making on IS of ADPS CA, the automated IM service management subsystem is implemented in ISMS. Accordingly, the estimate of the following criteria of quality monitoring of IM service functioning was performed [9]: the identity of functioning of ADPS CA with the set parameters – E_{af}, the survivability of ADPS CA during the computer intrusion – E_{ta}.

Evaluation of parameters E_{af} and E_{ta} is performed using the model, based on semi-Markov processes [4, 7]. An assumption was made, that these processes are formed for a usual ADPS on the base of E – network. The suggested model allows to take into account the probabilistic nature of transitions between states of ADPS, and also to take into account the selected technical means of information protection. In addition, distribution laws used in ADPS and time of transitions between these states of the system were analysed.

The formalization of decision-making procedure is designed as a mathematical programming task. In the course of its decision it is necessary to choose an alternative $al \in AL$ out of the plurality of *AL*. The following conditions must be met:

$$E_{af}(al) \to \max; \tag{8}$$

$$E_{ta}(al) \geq E_{\min ta}; \tag{9}$$

$$E_{fa}(al) \wedge E_{fa}(al) = 1 \tag{10}$$

where $E_{\min ta}$ – set according to the technical task on ADPS constant; *al* – the alternative, characterized by controlled service functioning parameters of IMS in ADPS CA.

4. RESULTS

During the simulation the influence of the controlled parameter P_{im} was analysed – the probability of IM service launch (for example, of the software and information support) during the next start-up procedure of the standard ADPS CA and its IS subsystem. At the same time, depending on the returned by sensors indications, caused by selecting the corresponding SP, the values of parameters of the next launch of the IM service are determined. For a model ADPS they define which part of the controlled information is verified for integrity. In algorithms of protection of IP in a typical MIP only the principal possibility of launching the IM service is revealed.

With the help of the developed programs complex [5, 6, 7] a complex study of the quality of functioning of a typical MIP from unauthorized access was carried out, with regard to the functioning of an automated working place on the base of a computer as a part of ADPS CA for a large railway unit.

The calculation results in the form of dependencies $E_{iaf}(P_{im})$ and $E_{ita}(P_{im})$, criteria E_{af} and E_{ta} on the controlled parameter P_{im} for different variants of SP and a typical MIP of ADPS CA are shown on the graphs. On the pictures 3 and 4 the curves $E_{iaf}(P_{im})$, $E_{ita}(P_{im})$ are different in values $\tau_{maf} = 3600(i+1)$ and $\tau_{mta} = 60i$ correspondingly, where τ_{maf}, τ_{mta} – average values of maximum permissible time intervals between adjacent integrity checks and implementation of MIP from unauthorized access of protective functions of ADPS CA. The increase in the parameters shown in the graphs, is interpreted as an improvement (by this criterion) of the quality of IM service operation. The decrease corresponds to the deterioration of indicators. Thus, on basis of the received dependencies, it is possible to make amendments in the algorithm of assessment of the current IS risk indicator – C_{ICR} [14, 15].

5. CONCLUSIONS

The following main results were obtained:

A model of the company's information security management system is proposed; it is found that the model makes it possible to assess the risks levels of the IS violation, as well as provides support for the decision to counter the unauthorized access to ADPS CA; algorithms are developed for the implementation of the proposed model, allowing to respond quickly and make decisions in case of threats to IS.

REFERENCES

[1] Akhmetov, B. etc. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 860, pp. 162–171.

[2] Lakhno, V., Zaitsev, S., Tkach, Y., Petrenko, T. (2019). Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, 754, pp. 673–682.

[3] Akhmetov, B., Balgabayeva, L., etc. (2019). Mobile platform for decision support system during mutual continuous investment in technology for smart city, Studies in Systems, Decision and Control, 199, pp. 731–742.

[4] Akhmetov, B., Lakhno, V., Akhmetov, B., Myakuhin, Y., Adranova, A., Kydyralina, L. (2019). Models and algorithms of vector optimization in selecting security measures for higher education institution's information learning environment, Advances in Intelligent Systems and Computing, 860, pp. 135–142.

[5] Lakhno, V., Kasatkin, D., Kozlovskyi, V., Petrovska, S., Boiko, Y., Kravchuk, P., Lishchynovska, N. (2019). A model and algorithm for detecting spyware in medical information systems, International Journal of Mechanical Engineering and Technology, (1), pp. 287–295.

[6] Lakhno, V., Tsiutsiura, S., Ryndych, Y., Blozva, A., Desiatko, A., Usov, Y., Kaznadiy, S. (2019). Optimization of information and communication transport systems protection tasks, International Journal of Civil Engineering and Technology, 10 (1), pp. 1–9.

[7] Lakhno, V., Buriachok, V., Parkhuts, L., Tarasova, H., Kydyralina, L., Skladannyi, P., Skrypnyk, M., Shostakovska, A. (2018). Development of a conceptual model of adaptive access rights management with using the apparatus of petri nets, International Journal of Civil Engineering and Technology, 9 (11), pp. 95–104.

[8] Akhmetov, B., etc. (2018). Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions, International Journal of Mechanical Engineering and Technology, 9 (10), pp. 1114–1122.

[9] Lakhno, V., Akhmetov, B., Korchenko, A., Alimseitova, Z., Grebenuk, V. (2018). Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity, Journal of Theoretical and Applied Information Technology, 96 (14), pp. 4530–4540.

[10] Akhmetov, B., Lakhno, V. (2018). System of decision support in weaklyformalized problems of transport cybersecurity ensuring, Journal of Theoretical and Applied Information Technology, 96 (8), pp. 2184–2196.

[11] Lakhno, V., Akhmetov, B., Malyukov, V., Kartbaev, T. (2018). Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium

of a bilinear multistep quality game with several terminal surfaces, International Journal of Electronics and Telecommunications, 64 (4), pp. 467–472.

[12] Lakhno, V.A., Kravchuk, P.U., Pleskach, V.L., Stepanenko, O.P., Tishchenko, R.V., Chernyshov, V.A. (2017). Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems, Journal of Theoretical and Applied Information Technology, 95 (8), pp. 1705–1714.

[13] Akhmetov, B. etc. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1 (2-85), pp. 4–15.

[14] Borowik, Bohdan, et al. Theory of Digital Automata. Vol. 63. Springer Science & Business Media, 2012.

[15] Smirniy, M., etc. (2009). The research of the conflict request threads in the data protection systems. Proceedings of Lugansk branch of the International Academy of Informatization, 2(20), pp. 23–30.

[16] Petrov, O., Borowik, B., Karpinskyy, M., etc. (2016). Immune and defensive corporate systems with intellectual identification of threats. Pszczyna: Śląska Oficyna DrukarskaGordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions On Information and System Security (TISSEC), 5(4), pp. 438–457.