Proceedings of

2020 7th International Conference on Electrical and Electronics Engineering (ICEEE 2020)

Antalya, Turkey

April 14-16, 2020

ISBN: 978-1-7281-6787-9

IEEE Catalog Number: CFP20M39-USB

2020 7th International Conference on Electrical and Electronics Engineering

Compliant PDF Files
IEEE Catalog Number: CFP20M39-ART
ISBN: 978-1-7281-6788-6

Conference USB
IEEE Catalog Number: CFP20M39-USB
ISBN: 978-1-7281-6787-9

Additional copies of this publication are available from

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
+1 845 758 0400
+1 845 758 2633 (FAX)
email: curran@proceedings.com

Publisher: Institute of Electrical and Electronics Engineers, Inc.

Printed in Antalya, Turkey

2020 7th International Conference on Electrical and Electronics Engineering (ICEEE 2020)

Table of Contents

Expert System for Assessing the Efficiency of Information Security

Aizhan Erulanova
School of engineering
D. Serikbaev East Kazakhstan State Technical University
Oskemen, Kazakhstan
e-mail: A_Erulanova@BK.ru

Gulzhan Soltan
Information Technology department
S.Seifullin Kazakh Agro Technical University
Nur-Sultan, Kazakhstan
e-mail: gsoltan@mail.ru

Aizhan Baidildina
School of engineering
D. Serikbaev East Kazakhstan State Technical University
Oskemen, Kazakhstan
e-mail: atj-43@mail.ru, azhaparova@ektu.kz

Marzhan Amangeldina
Information Technology department
I. Razzakov Kyrgyz State Technical University
Bishkek, Kyrgyzstan
e-mail: marzhanamangeldina@mail.ru

Askhat Aset
Subject Cycle Commission
Innovative Technical College of Almaty
Almaty, Kazakhstan
e-mail: Aset.asxat@mail.ru

***Abstract*—The paper considers an expert system that provides an assessment of the state of information security in authorities and organizations of various forms of ownership. The proposed expert system allows to evaluate the state of compliance with the requirements of both organizational and technical measures to ensure the protection of information, as well as the level of compliance with the requirements of the information protection system in general. The expert assessment method is used as a basic method for assessing the state of information protection. The developed expert system provides a significant reduction in routine operations during the audit of information security. The results of the assessment are presented quite clearly and provide an opportunity for the leadership of the authorities and organizations to make informed decisions to further improve the information protection system.**

Keywords-information security; authorities; protected information; information system; coefficient of significance; organizational and administrative documents; personal data; audit information security

I. INTRODUCTION

The necessity to develop an expert system (ES) to assess the efficiency of information security is due to a number of circumstances [1-3].

Due to the large amount of source data, cumbersome processing procedures, the complexity of making decisions about the state of information security in organizations in a large number of factors taken into account, it is almost impossible to carry out the necessary assessments without automating this process [4-5]. Automation, in fact, leads to the creation of an appropriate expert system that implements automated decision support in conducting assessments of the state of information security.

In the process of assessing the state of information security and trends of its change, as a rule, an analysis of the influence of significant factors (parameters, characteristics and conditions of information systems) on the results of the assessment is carried out [6-8]. It should be noted that the need for such an analysis significantly complicates the requirements for the ES.

If we dwell only on the procedures for collecting data and assessing the state of information security, it would be sufficient to develop an appropriate database and program for calculating indicators. However, in practice it is necessary not only to assess the state of information security, but also to establish the factors, the change of which will increase the security of information systems from destructive information impacts.

Such an analysis could be carried out on the basis of multiple calculations of indicators for evaluating information security according to the developed analytical ratios, however, it is necessary to vary a large number of individual indicators used in the calculations of complex performance indicators. An important role in assessing the state of information security is the assignment of weights to indicators of all levels, which is usually carried out using expert survey methods, which leads to deviations in the results of the assessment and the need to adjust the weights of the indicators [9-10]. The results of expert evaluation largely depend on the method used, but in any case, these procedures are quite routine.

In the presence of incomplete or fuzzy source data, the results of previously conducted analyzes of the state of information security can be an important help, but time-

consuming procedures for comparing numerous source data make it extremely difficult to use direct methods for calculating indicators in the interests of such analysis [11-12]. The proposed expert system is a specialized software product installed on automated workplaces of both specialists responsible for ensuring information security and managers of an organization.

II. Stages of Performance Evaluation

The expert system provides the ability to assess the effectiveness of information protection at the pre-design stage of creating information protection systems when conducting an internal (external) information security audit to determine whether information systems comply with information security requirements [13-15].

Work on assessing the effectiveness of information security is carried out by performing the following procedures:

- Stage 1 - preparation of the initial data;
- Stage 2 - monitoring the implementation of requirements;
- Stage 3 - calculation of integrated indicators for assessing the state of the information protection system (IPS).

A. The Stage of Preparation of the Initial Data

At stage 1, the following source data is prepared:

- The list of types of protected information {hi} (the main types of protected information are: information containing information constituting state secrets, proprietary information, personal data, publicly available information);
- Lists of requirements for the composition of organizational and administrative documents (OAD) set forth in regulatory acts {pra} and regulatory documents {prd} in the field of information security [16] (requirements tables are generated for each type of protected information);
- Lists of requirements for information security units {ps} and qualifications of employees of these units {ps} [17];
- List of types of information systems {δ};
- A list of requirements for IPS information systems and IPS information systems of personal data, as well as the level of personal data security { pfp };
- Classes of security of information systems { qis };
- Types of information systems operating in the organization;
- The number of information systems of each type.

B. Stage of Monitoring the Implementation of Requirements

In stage 2, the following activities are carried out:

Step 1. Formation of questionnaires for monitoring the implementation of requirements.

Step 2. Directly monitoring the implementation of the requirements, carried out by the method of questioning. Taking into account the information available in the database, the input data, the following questionnaires are automatically generated.

- Questionnaire requirements for the composition of the OSA, set out in regulatory legal acts;
- Questionnaire requirements for the composition of the OSA, set out in the regulatory documents in the field of information protection;
- Questionnaire of requirements for the qualification level of specialists of the unit providing information security in the organization;
- Questionnaire requirements for the composition of departments, specialists, providing information security;
- Questionnaire requirements for the information system information protection system.

These requirements are determined taking into account the class of protection of the information system and the basic set of requirements for the information security system of the information system. The number of questionnaires with the requirements for information security systems of information systems corresponds to the number of information systems operating in the organization [18-19].

Step 3. Monitoring the implementation of the requirements is carried out by members of the commission responsible for ensuring information security in the organization. In the course of the control, the fulfillment of the requirements for each questionnaire is checked, and in the column “Single indicators, actual fulfillment”, “1” is put down if the requirement is met and “0” otherwise.

C. The Stage of Calculation of Complex Indicators for Assessing the State of the Information Protection System

The degree of fulfillment of requirements for each functional subsystem $W_r^{\Pi i}$ is calculated from the dependence of formula (1):

$$W_r^{\text{пі}} = \frac{\sum_h p_{rh}^{\text{фпі}}}{\sum_h p_{rh}^{\text{тпі}}},\ 0 \le W_r^{\Pi i} \le 1 \qquad (1)$$

where $p_{rh}^{\text{тпі}}$ is the required value of a single indicator, r = 1: R is the number of functional subsystems in the IPS of the i-th IS, h = 1: H_r, H_r is the number of unit requirements for the r-th functional subsystem of the IPS of the i-th information system.

The value of Hr depends on the IS security class (level of personal data security); $p_{rh}^{\text{фпі}}$ - the actual implementation of the h-th requirement in the r-th functional subsystem of the i-th information system. The calculation of the complex indicator of the degree of fulfillment of the requirements for the composition of the OSA set forth in the normative documents in the field of PF –$W^{\text{НД}}$= F ($p_n^{\text{нд}}$), is carried out taking into account the following dependence of formula (2):

$$W^{\text{нд}} = \frac{\sum_n p_n^{\text{фнд}}}{\sum_n p_n^{\text{тнд}}},\ 0 \le W^{\text{нд}} \le 1 \qquad (2)$$

where $p_n^{\text{фнд}}$, $p_n^{\text{тнд}}$ are the requirements for the composition of the OSA set forth in the normative documents in the field of IS, and their actual fulfillment. A comprehensive indicator of the degree of fulfillment of the requirements for the

composition of the OSA set forth in regulatory legal acts – W^{RA}, is calculated using the formula (3):

$$W^{\text{НП}} = \frac{\sum_s p_s^{\text{ФНП}}}{\sum_s p_s^{\text{ТНП}}}, \quad 0 \leq W^{\text{НП}} \leq 1 \qquad (3)$$

where $p_s^{\text{ФНП}}$, $p_s^{\text{ТНП}}$ - requirements for the development of the document required in accordance with the requirements of the regulatory framework in the field of IS, and its actual implementation. The calculation of the complex indicator of the degree of fulfillment of the requirements for the structure and composition of the information security unit – W^{C} == F (p_m^{C}) is performed as follows using formula (4):

$$W^{C} = \frac{\sum_m p_m^{\text{ФС}}}{\sum_m p_m^{\text{ТС}}} \; 0 \leq W^{C} \leq 1 \qquad (4)$$

where $p_m^{\text{ТС}}$, $p_m^{\text{ФС}}$ are the requirements for the structure and composition of the information security unit and their actual implementation. The complex indicator of the degree of fulfillment of the requirements for the qualifications of information security department specialists - W^{K} == F (p_q^{k}) - is calculated from the dependence of formula (5):

$$W^{K} = \frac{\sum_q p_q^{\text{ФК}}}{\sum_q p_q^{\text{ТК}}}, \quad 0 \leq W^{K} \leq 1 \qquad (5)$$

where p_q^{TK}, $p_q^{\text{ФК}}$ are the requirements for the qualifications of the information security department's specialists and their actual fulfillment.

III. Algorithmization of the Process of Calculating a Comprehensive Indicator of the Efficiency of Information Security Measures

The calculation of performance indicators is carried out in accordance with the algorithm shown in Fig. 1. The expert system is implemented as a software product for which there is a certificate of state registration of computer programs. The sequence of work using the expert system is shown in Fig. 2. Experimental studies of the state of information security assessment (ISA) program (ISMS) were carried out using the principles of unit testing. In the course of conducting experimental studies, it was determined that the algorithm for assessing the degree of fulfillment of requirements has such essential properties as discreteness, determinism, finiteness, and effectiveness.

In the expert system, it is assumed that all functional subsystems R have the same effect on the fulfillment of the requirements of IPS IS. Therefore, the complex indicators of the degree of fulfillment of the requirements for IPS for IS, functioning in an organization - W_i^{IS} - are calculated by formula (6):

$$W^{\text{ИСi}} = \frac{\sum_r p_r^{\text{П}i}}{R}, \quad 0 \leq W^{\text{ИСi}} \leq 1 \qquad (6)$$

where r = 1: R, R is the number of functional subsystems in the IPS of the i-th IS. The next step is the calculation of complex indicators characterizing the degree of implementation of organizational, legal and technical measures to protect information in the organization.

A complex indicator to organizational measures to protect information W^{O}= F (W^{C}, W^{K}) is calculated by the formula (7):

$$W^{O} = \frac{\sum_m p_m^{\text{ФС}} + \sum_q p_q^{\text{ФК}}}{\sum_m p_m^{\text{ТС}} + \sum_q p_q^{\text{ТК}}}, \; 0 \leq W^{O} \leq 1 \qquad (7)$$

In a similar way, a complex indicator of the degree of fulfillment of the requirements for legal measures of IS $W^{\text{П}}$ = F ($W^{\text{НП}}$, $W^{\text{НД}}$) is calculated.

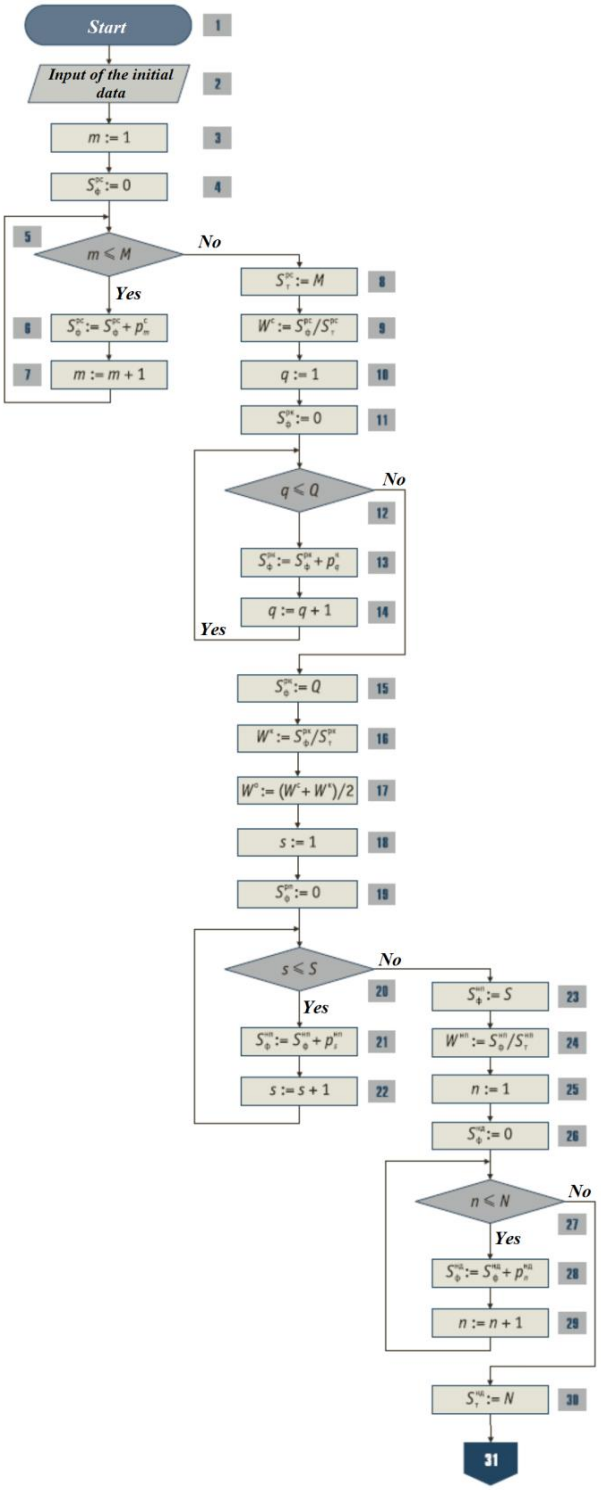

Figure 1. First half of algorithm for calculating performance indicators

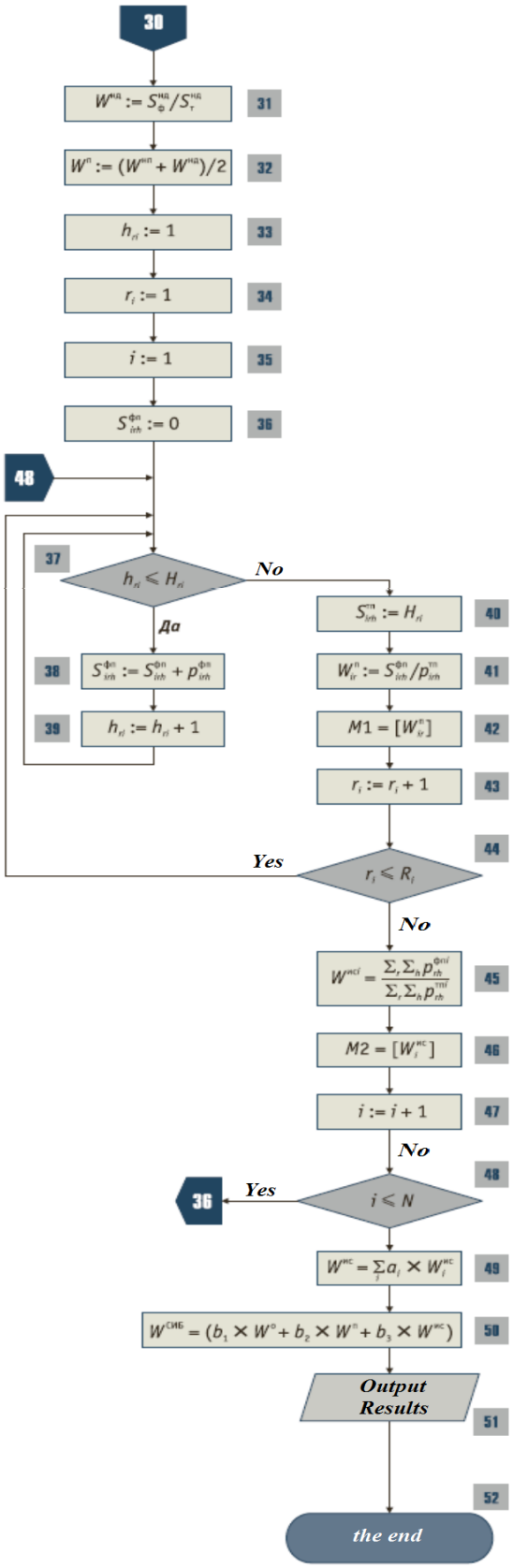

Figure 2. Second half of algorithm for calculating performance indicators

When calculating the complex indicator of the effectiveness of technical measures to protect information in the information system - W^{IS} = F (W_i^{IS})- it is necessary to take into account that information about limited access of different confidentiality levels is being processed, as previously indicated. Violations of IS protection, processing information of various types of confidentiality, have different significance in the formation of a complex indicator - W^{IS}. Taking into account the above, when calculating the indicator, weighting coefficients of the IS are introduced, the complex indicator W^{IS} is calculated by the formula (8):

$$W^{IS} = \sum_i a_i * W_i^{IS}, 0 \le W^{IS} \le 1 \qquad (8)$$

where a_i is the coefficient of significance of the i-th IS (W_i^{IS}), $\Sigma\, a_i = 1$.

The final step in evaluating the effectiveness is the calculation of the complex indicator W^{ISS}. When calculating W^{ISS}, the degree of fulfillment of requirements on protected IS (W^{IS}), degree of fulfillment of organizational (W^{O}) and legal (W^{L}) requirements in the interests of ensuring information security in the organization are taken into account.

The contribution of each indicator to the provision of information security is of different weights, so W^{ISS} is calculated using the formula (9):

$$W^{ISS} = b_1 * W^{O} + b_2 * W^{L} + b_3 * W^{IS}, \qquad 0 \le W^{ISS} \le 1, \qquad (9)$$

where b1, b2, b3 are the coefficients of significance of the indicators W^{O}, W^{L} and W^{IS}, respectively, b1 + b2 + b3 = 1.

The coefficients of significance a_i, b1, b2, b3 are determined taking into account the recommendations based on the results of an expert survey [20-22]. The sequence of work using the expert system is shown in Fig. 3.

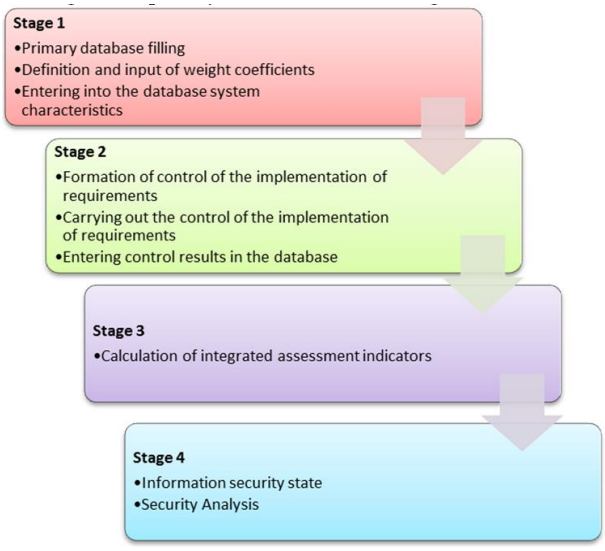

Figure 3. The sequence of work using the expert system

It is established that the developed program ISA ISMS after testing and debugging:

- Provides the correct results for solving the problem;
- Has a low probability of failure in the process of solving the problem;
- Provides sufficient performance for solving the problem;
- Meets the requirements of practicality (applicability).

IV. CONCLUSION

Thus, it can be concluded that the proposed mathematical model, algorithm and program can be used in the practical activities of the units responsible for the security of information. The described expert system, unlike the existing ones, allows you to perform rapid assessment of the state of information security of authorities and organizations during an information security audit, while periodically monitoring the effectiveness of information security, automate the process of developing recommendations for improving the organization's information security system, and also provides a solution to assessment tasks and analysis of the state of information security systems.

REFERENCES

[1] Fayoumi, A., & Loucopoulos, P. (2016). Conceptual modeling for the design of intelligent and emergent information systems. Expert Systems with Applications, 59, 174-194.

[2] Uvalieva, I., & Smailova, S. (2014, October). Development of decision support system to control the quality of education. In 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-6). IEEE. DOI: 10.1109/ICAICT.2014.7036018

[3] Saule, K., Indira, U., Aleksander, B., Gulnaz, Z., Zhanl, M., Madina, I., & Györök, G. (2018). Development of the Information and Analytical System in the Control of Management of University Scientific and Educational Activities. Acta Polytechnica Hungarica, 15(4), 27-44.. DOI: 10.12700/APH.15.4.2018.4.2

[4] Grover, V., Chiang, R. H., Liang, T. P., & Zhang, D. (2018). Creating strategic business value from big data analytics: A research framework. Journal of Management Information Systems, 35(2), 388-423.

[5] Wang, H., Xu, Z., Fujita, H., & Liu, S. (2016). Towards felicitous decision making: An overview on challenges and trends of Big Data. Information Sciences, 367, 747-765.

[6] Uvalieva, I., Garifullina, Z., Utegenova, A., Toibayeva, S., & Issin, B. (2015, May). Development of intelligent system to support management decision-making in education. In 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) (pp. 1-7). IEEE. DOI: 10.1109/ICMSAO.2015.7152249

[7] Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2017, July). A security metric catalogue for cloud applications. In Conference on Complex, Intelligent, and Software Intensive Systems (pp. 854-863). Springer, Cham.

[8] Bertino, E. (2015, June). Big data-security and privacy. In 2015 IEEE International Congress on Big Data (pp. 757-761). IEEE.

[9] Uvalieva, I., Turganbayev, E., & Tarifa, F. (2014, December). Development of information system for monitoring of objects of education on the basis of intelligent technology: a case study of Kazakhstan. In 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA) (pp. 909-914). IEEE.. DOI: 10.1109/STA.2014.7086779

[10] Cavelty, M. D., & Mauer, V. (2016). Power and security in the information age: Investigating the role of the state in cyberspace. Routledge.

[11] Naik, N., Jenkins, P., Savage, N., & Katos, V. (2016, December). Big data security analysis approach using computational intelligence techniques in R for desktop users. In 2016 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-8). IEEE.

[12] Elnajjar, A. E. A., & Naser, S. S. A. (2017). DES-Tutor: An Intelligent Tutoring System for Teaching DES Information Security Algorithm.

[13] Sehgal, V. K., Patrick, A., Soni, A., & Rajput, L. (2015). Smart human security framework using internet of things, cloud and fog computing. In Intelligent distributed computing (pp. 251-263). Springer, Cham.

[14] Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016, June). Big data analytics: Security and privacy challenges. In 2016 IEEE Symposium on Computers and Communication (ISCC) (pp. 952-957). IEEE.

[15] Holm, H., & Afridi, K. K. (2015). An expert-based investigation of the common vulnerability scoring system. Computers & Security, 53, 18-30.

[16] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

[17] Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31(2), 243-256.

[18] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

[19] Saini, S., Beniwal, R. K., Kumar, R., Paul, R., & Saini, S. (2018). Modelling for improved cyber security in Smart distribution system. International Journal on Future Revolution in Computer Science & Communication Engineering, Accepted.

[20] Belginova, S., Uvaliyeva, I., & Ismukhamedova, A. (2018, May). Decision support system for diagnosing anemia. In 2018 4th International Conference on Computer and Technology Applications (ICCTA) (pp. 211-215). IEEE.

[21] AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575.

[22] Kubekov, B., Baidildina, A., Utegenova, A., & Erulanova, A. (2019, June). Implementation of analytical distributed monitoring of education system. In Proceedings of the 5th International Conference on Engineering and MIS (pp. 1-5).

ISBN : 978-1-7281-6787-9
IEEE Catalog Number : CFP20M39-USB

2020 7th International Conference on Electrical and Electronics Engineering (ICEEE 2020)

ISBN : 978-1-7281-6787-9

ICEEE 2020

2020 7th International Conference on Electrical and Electronics Engineering

Antalya, Turkey | April 14-16, 2020

Co-supported by 1982 Üniversitesi IEEE Turkey Section

Published by IEEE