Analysis of Cyber Security Threats of the Printing Enterprise

Petro Shepita*, Lyubov Tupychak
and Julia Shepita

Department of Computer Sciences & Information Technologies, Ukrainian Academy of Printing, Lviv, Ukraine
E-mail: pshepita@gmail.com; ltupychak@gmail.com; vitrivulia@gmail.com
**Corresponding Author*

Received 31 October 2022; Accepted 14 February 2023;
Publication 16 May 2023

Abstract

The topic of scientific works on the implementation of modern technologies and systems of automated management of the enterprise, its resources and technical means is analyzed, and the insufficient completeness of research on the features of the integrated approach to the design and deployment of innovative means of production order support. Based on the determined factors of the operation of the enterprise in the latest conditions of the fourth industrial revolution, directions for the formation of strategies for the introduction of the elements of Industry 4.0 in modern printing enterprises, as well as information protection systems, are determined with electronic document circulation. The mechanisms of decision of tasks of management informative risks considered in complex control system by printeries in the conditions of vagueness and at co-operation of elements of control system between itself. The necessity of using a web portal for the formation of printing orders is substantiate, the main components are define and the

Journal of Cyber Security and Mobility, Vol. 12_3, 415–434.
doi: 10.13052/jcsm2245-1439.123.8

levels of access to them described. The paper examines the use of classic and gray fuzzy cognitive maps to solve the problem of cyber security risk assessment of the intelligent management system of a printing enterprise. It is demonstrate that the average estimate of local risk, which is formed using an ensemble of two heterogeneous fuzzy cognitive maps, decreases compared to the use of individual cognitive maps. In order tî better, highlight the results of the research, an example of the application of the proposed methodology for assessing the risks of ensuring the integrity of telemetric information in the industrial network of the intelligent technological process management system of a printing enterprise given, with the continuity of the technological process of manufacturing printing products. In addition to the classic FCM, the paradigms of two variants of the FCM extension were also use in the study, namely, the gray FCM, which used to solve the problem of assessing cyber security risks of intelligent management systems of printing enterprises. An analysis of the possibility of building FCM ensembles to increase the effectiveness of risk assessment using several options for formalizing the expert's knowledge and experience performed. A fragment of the enterprise management system was consider and an analysis of possible directions of attacks on the printing enterprise by malicious software was perform. These are attacks such as replacing the executable files of server and ARM software, overwriting PLC projects during system operation, and refusing to service the equipment. Based on the formed list of attack vectors and the consequences of their implementation, the task of analyzing the risks of cyber security of a printing enterprise, taking into account the impact on the system of possible internal threats, was considered, using the cognitive modeling apparatus as a modeling tool. The scenario of cognitive modeling of the influence of an internal criminal who exploits the vulnerabilities of the software and hardware components of the control system using the given variants of FCM construction is considered. The average assessment of local risks, which formed using an ensemble of cognitive maps, is better from the point of view of dispersion of assessments of the state of target concepts than the use of individual FCMs. The spread of estimates of the state of ensemble concepts is smaller than the spread of estimates of their gray values using the GFCM, on average by 1.4–1.8 times, which indicates a decrease in the influence of the subjectivity factor on the results of risk assessment. The performed scenario modeling showed that the use of the specified means of protection and organizational measures allows reducing the assessment of local risks by 12–18%, which is a significant indicator. This technique allows obtaining a qualitative and quantitative assessment of

risk indicators, taking into account the entire set of objective and subjective factors of uncertainty.

Keywords: FCM, ICS, cyber security, printing company, cognitive modeling cognitive map, technological process.

1 Introduction

One of the indispensable conditions for building an effective digital economy is ensuring the reliable and safe operation of intelligent control systems for complex technological processes (ISU), which is the basis of the production cycle at modern industrial enterprises. At the same time, as the statistics of recent years show, the number of cases related to attempts or successful implementation of targeted attacks on computers of ISU has increased sharply.

Automation and protection of information at printing enterprises is a rather complex and long-term process, which has been improved for decades since the appearance of the first elements of automation in order to systematically improve the quality of manufactured products, speed up their production and reduce production costs, increase production capacity. At the current stage of information technology development, the automated control system, under the influence of the fourth industrial revolution, is moving into the category of an intelligent system, which involves autonomous work without human intervention. Within these projects, a large number of large-scale distributed systems are created, which often have no analogues both in their complexity, on the one hand, and in terms of the size of potential threats that arise in the event of their failure or incorrect operation, on the other hand. Thus, the problem of ensuring information security and risk management of complex systems is becoming more relevant than ever. Moreover, this applies not only to the active implementation of existing methods and means of risk management, but also to their improvement and development of new approaches to solving the specified problems using logical and cognitive approaches.

In recent years, the rapid development of artificial intelligence technologies, machine learning and big data processing have reached a high level of integration into people's lives and the everyday production processes of large companies, including printing companies [1], and technological and informational production processes are constantly under real-time control [2]. The integrated integration of production control systems, physical sensors

and executive mechanisms in the digital space significantly improves the productivity of the enterprise, but at the same time creates new threats to the security of control systems. Timely detection of malicious intrusions is the basis of modern approaches to building a cyber defense system. Ukrainian and international scientists pay a lot of attention to researching ways and means of detecting network intrusions.

Detection in the protection against intrusions of the management system of a printing company consists in the collection and analytical study of the behavior of the system in the enterprise's corporate network and is compared with known patterns of intrusion behavior or atypical behavior of the management system, in order to detect interference in the operation of the system [3].

Thus, according to data from international companies, the total percentage of industrial computers in the world on which malicious software was detected and blocked in the first half of 2021 was 42%, i.e. almost every second computer has been attacked. Enterprises in the energy, engineering, oil and gas sector and other equally important industries were equally exposed to attacks, which certainly indicates the acuteness of the emerging situation and the need to take urgent steps to improve it.

2 Overview of the Main Aspects of the Theory of Fuzzy Cognitive Maps

Conducted research on this subject is devoted to the protection of information during electronic document circulation at printing enterprises and publishing houses [4, 5]. However, when designing intellectual management for printing enterprises, which is considered in publications [6, 7], it is necessary to take into account the security of the information system operating in the automatic order processing mode. With normal document circulation, it is sufficient to ensure the protection described in the publication [8]. However, the intelligent system that interacts with the customer directly through the web portal is exposed to external factors, to prevent which there is a need for thorough research.

The approach to solving the given task, when the specific type of local risk functions is unknown, was first outlined, albeit in a slightly different formulation, in the article [9], and most fully explained in the monographs [10, 11]. Works [12–15] describe the process of building an information protection and cyber security system using deep and machine learning according to the system and cognitive method.

The basis of the classic approach to solving cyber security issues prescribed in regulatory documents is the methodology of a systemic risk-oriented approach to ensuring cyber security of the ISU [16, 17]. From an ideological point of view, this methodology is close to recent years, and was called the cognitive modeling methodology, the essence of which is the construction and further analysis of fuzzy cognitive maps (Fuzzy Cognitive Maps, FCM) using the knowledge and experience of experts in the analyzed problem area [18, 19, 35–37].

According to the definition of B. Kosko [20], a fuzzy cognitive map (FCM) is a directed graph defined by a tuple of sets.

$$Fcm = \langle C, F, W \rangle, \tag{1}$$

where $C = \{C_i\}$ is a set of concepts of graph vertices, which are represented as factors, the value of which is the most significant for the selected type of management system. $F = \{F_k\}$ is the set of true arcs of the graph that connect concepts; $W = \{W_{ij}\}$ is the set of all available *FCM* connections, which can be both negative and positive, thus strengthening or weakening the influence of concept C_i on concept C_j.

We set the value of the weight coefficients W_{ij} using a fuzzy linguistic scale, which represented in the form of ordered set terms. Each of the given values of linguistic variables is contrasted with a certain numerical range, which, depending on the type of connection, lies within $[-1, 1]$ (Table 1).

In order to describe the state of the *FCM* at a random discrete moment in time, we use Equation (2)

$$X_i(t+1) = f\left(X_i(t) + \sum_{j=1, j\neq i}^{n} W_{ji} X_j(t)\right) \quad where\ (i = 1, 2, \ldots n) \tag{2}$$

Table 1 Evaluative reflection of the strength of connections between concepts

Value	Conventional Designation	Range	Impact Assessment
Does not affect	NW	0	0,000
Minimal impact	WL	[0; 0.17]	0.100
Weak influence	L	[0.17; 0.37]	0.260
Medium impact	M	[0.37; 0.62]	0.480
Strong influence	H	[0.62; 0.85]	0.740
Maximum impact	MW	[0.85; 1]	0.985

where $X_i(t)$ is the value of the state variable i of the concept C_i at the moment of time t. $X_i(t+1)$ is the value of the same variable at the moment of time $(t+1)$. n – number of selected concepts within the printing enterprise. f – activation function (within the concept of a printing company, the selected function is the hyperbolic tangent).

Given the initial conditions and using formula (2), we calculate the state variables $\mathrm{X_i(t)}$.

Without dwelling in detail on the question of choosing the composition of FCM concepts and the list of their relationships (a similar task discussed, for example, in [8]), we note that the task of evaluating the strength of connections (weights) of FCM is no less important. As possible ways to solve this problem, a number of authors proposed special constructions (extensions) of FCM related to presenting the strength of FCM connections in the form of some interval estimates. Such FCM structures include such varieties of FCM as Gray FCM) [21], Interval-Valued FCM [22], Rough FCM [20], Intuitionistic FCM [24].

In addition to the classical FCM, the paradigms of two variants of the FCM expansion were also use in the research, namely the gray FCM, which was used to solve the problem of assessing cyber security risks of intelligent control systems of printing enterprises. Of particular interest is the analysis of the possibility of building FCM ensembles to increase the effectiveness of risk assessment using several options for formalizing the expert's knowledge and experience. This issue is partially considered in the works [25–27], devoted mainly to the use of these cognitive models in the construction of attack detection systems and the assessment of information risks associated with them, but the issue of intelligent management systems in highly specialized industries, such as for example, the printing industry.

3 Using the Apparatus of Fuzzy Cognitive Maps to Assess Cyber Security Risks at a Printing Company

As an object of protection under investigation, we consider the intelligent management system of a printing company at the stage of receiving an order, online coordination of processes in production shops, and online exchange of administrative data.

Clients who log in to the system get access to the external part (site) to place orders and track their fulfillment. This function is implemented through the customer's personal account [28].

The administrative part of the platform provides communication between employees, the management system, and the client (customer). In addition, it allows generating tags to form a parametric description of order fulfillment [12]. Since there is a large amount of important production and corporate data in the system, it suggested duplicate them on a backup server.

Thus, foreseen design of online platform times, construction of administrative part of dynamic web service for the reflection of information of monitoring and watching of the stages of performing the orders it is uncommunicative in the presented research as base modules of corporate web platform. a project is for high-quality and operative implementation of separate shallow orders, and also large orders [29].

Based on the justification of the need to use an online service for the presentation of printing products and building a series of user interactions of different profiles, the design of the order formation model performed, the central element of which is the web user interface that interacts with the customer, employee and manager.

User profiling allows you to grant different rights and opportunities depending on the access rights, the activation of such functions reduces the load and server resources of the enterprise. For this purpose, four main categories of users who have access to the modules of the online platform are introduced into the model. The guest customer is located in this hierarchy of users at the bottom level, since he has the least access rights and only got on the platform to create the first order. In this regard, he does not yet have the possibility of tracking the order in real time, as well as direct communication with the consultant's personal consultant, unlike the customer (registered user). Creating a personal account provides an opportunity on the web interface to open the function of tracking the systematic passage of an order through the production stages of a printing company. It is also possible to track finished products that are packaged and sent to the client. The personal office provides opportunities for online layout, selection of materials and type of products for the formation of a production order. In real time, the cost of the order is calculate based on the selected parameters, and depending on the workload of the production and the raw materials available in the warehouse, the terms of the order are calculated. The customer optionally gives his consent to receive notifications about the stages of the order; this allows increasing customer information and reducing the burden on operator managers who are responsible for customer feedback [30, 31].

The employee profile allows the qualified staff of the printing company to connect together to the company's management system using the Internet,

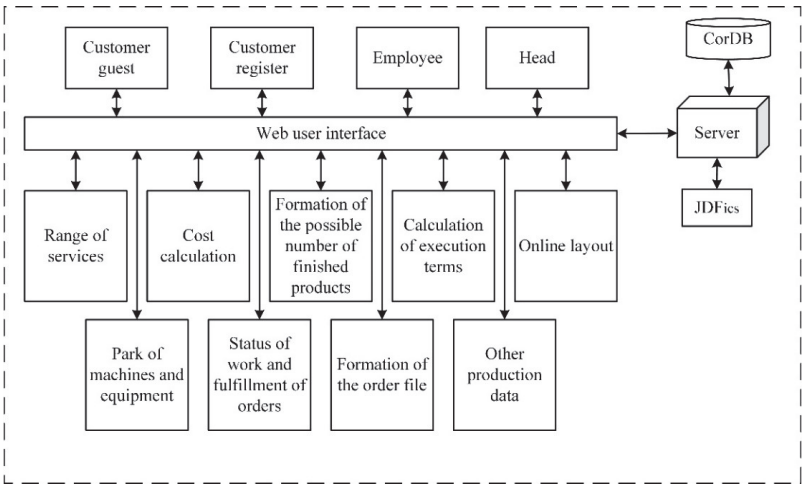

Figure 1 Model of order formation in the intelligent management system of a printing company.

which allows remote measurement and debugging of devices and work process units. However, an important component characteristic of the employee's profile is the monitoring of the company's equipment and resources. Since the qualified personnel in the section of the enterprise also includes administrative blocks that have only a tangential relationship to the production shop, such as: accounting, personnel department, warehouse, etc., internal profiling of employees is also provided for, which correlates with their functions at the printing enterprise [32].

The profile of the manager allocated in a separate block; this related to the type of profile, as it has an analytical purpose. Allows you to view order statistics, the number of completed orders, the number of orders in progress and various administrative parameters that the company manager needs.

Communication of all levels of users takes place through the web user interface, which connected through the server of the enterprise with the corporate database. Such an organization allows combining various parameters of the production cycle, administrative protocols. The range of services block certifies the types of products that can manufactured by the enterprise using equipment, the list of which is located in the machine and equipment park block. The employee and manager user profiles have access to the equipment list. The presence of such a segment in the online platform allows monitoring the condition of the equipment and provides the possibility of its configuration and remote reconfiguration [33].

The cost calculation serves for the client as an information source about the cost of the finished product of his choice, and its estimated date of manufacture realized in the block of calculation of execution terms. An important step in the operation of the web service is the formation of the order and the loading of the layout. This stage propose implemented in two ways: the first is to download the finished layout through a window in the user's personal account; the second involves creating a layout online using layout tools in your personal account. To transfer data that is specialized and structured on the online platform, the *JDFics* file container introduced into the model of the order formation process, which transfers the data to the next stage of the order process and is a modified version of *JDF* [34].

On the basis considered fragment of the enterprise management system, an analysis of possible directions of attacks on the printing enterprise by malicious software performed. Basically, these attacks such as replacing the executable files of server and *ARM* software, overwriting *PLC* projects during system operation, and refusing to service the equipment.

Based on the formed list of attack vectors and the consequences of their implementation, we will consider the task of analyzing the risks of cyber security of a printing enterprise, taking into account the impact on the system of possible internal threats, using the cognitive modeling apparatus as a modeling tool.

The cognitive map for assessing the cyber security risks of the ICS of the printing company presented in Figure 2. The main concepts of the cognitive map given in Table 2.

Will consider two variants of FCM implementation (ordinary FCM and gray FCM). Table 3 shows the values of the weight of connections between concepts determined by experts.

Will consider the scenario of cognitive modeling of the influence of an internal criminal who exploits the vulnerabilities of the software and hardware components of the control system using the given options for building the FCM.

Taking into account generalized classical FCMs, we believe that the state equation of the FCM (1) will have the following form in its general form:

$$X_i(t+1) = f\left(X_i(t) \oplus \left(\bigoplus_{j=1, j\neq i}^{n} W_{ji} \otimes X_j(t)\right)\right)$$
$$where\ (i = 1, 2, \ldots n) \tag{3}$$

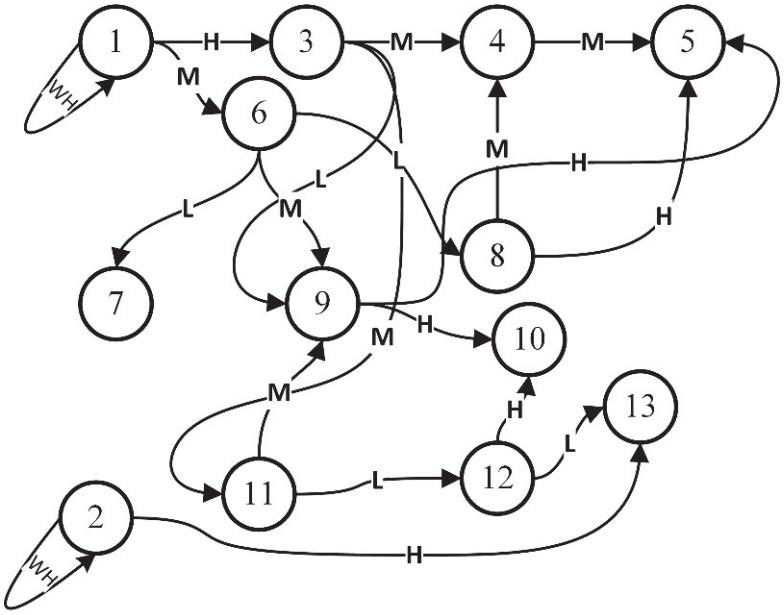

Figure 2 A cognitive map for assessing the cyber security risks of ICS.

Table 2 List of concepts of the cognitive map of the analysis of cyber security risks of an industrial facility

C_1	The influence of an insider
C_2	The impact of an external attacker Physical access to the operator's ATM
C_3	Authorization with the rights of a legitimate user of the system
C_4	Unauthorized control of the printing station. Target concept (X5).
C_5	Exploitation of network equipment vulnerabilities and/or configuration errors.
C_6	Failure to maintain the network of the lower level controllers of the industrial facility. Target concept (X7).
C_7	Filtering network traffic and intercepting user account data
C_8	Changing the management algorithm of objects of the industrial system due to modification
C_9	PLC configuration files (using HTTP + FTP protocols)
C_{10}	Violation of the logic of the printing company's work. Target concept (X10).
C_{11}	Access to the OS via SSH/Telnet protocols (exploitation of remote access vulnerabilities)
C_{12}	Exploiting vulnerabilities of equipment parameter collection sensors and replacing configuration files
C_{13}	Modification of vital properties of telemetry (integrity violation). Target concept (X13).

Table 3 Weights of connections between FCM concepts

Connection Weight $C_i \to C_j$	Conventional (Classical) FCM	Gray FCM
W_{ij}	W_{ij}	$[\underline{W_{ij}},\ \overline{W_{ij}}]$
W_{11}	1	[1;1]
W_{13}	0.740	[0.62; 0.85]
W_{16}	0.480	[0.37; 0.62]
W_{22}	1	[1;1]
$W_{2\ 13}$	0.260	[0.17; 0.37]
W_{34}	0.480	[0.37; 0.62]
W_{39}	0.480	[0.37; 0.62]
$W_{3\ 11}$	0.480	[0.37; 0.62]
W_{45}	0.480	[0.37; 0.62]
W_{67}	0.260	[0.17; 0.37]
W_{68}	0.260	[0.17; 0.37]
W_{69}	0.480	[0.37; 0.62]
W_{84}	0.480	[0.37; 0.62]
W_{85}	0.740	[0.62; 0.85]
W_{95}	0.740	[0.62; 0.85]
$W_{9\ 10}$	0.740	[0.62; 0.85]
$W_{11\ 9}$	0.260	[0.17; 0.37]
$W_{11\ 12}$	0.260	[0.17; 0.37]
$W_{12\ 10}$	0.740	[0.62; 0.85]
$W_{12\ 13}$	0.260	[0.17; 0.37]

where W_i, $X_i(t+1)$, $X_i(t)$ – interval numbers that are elements of interval sets.

As a basis for the construction of *FCM*, various methods of problem of interval fuzzy sets can be use. Gray *FCM* (*GFCM*) A gray set $A \subseteq X$ is a set

$$A = \{\langle x, [\underline{x}, \overline{x}]\rangle | x \in X\} \tag{4}$$

The elements of this set are gray numbers $x \in [\underline{x}, \overline{x}] \leq A$, that is, numbers that can take on any values within a certain range $[\underline{x}, \overline{x}] \in [0, 1]$, where x is the lower and upper limit of the gray number, respectively; *X* is a universal set.

The weights of connections between gray FCM concepts given in the form of gray numbers $[\underline{W_{ij}}, \overline{W_{ij}}]$; variable states of concepts are also gray numbers $[\underline{X_i}, \overline{X_i}]$ calculated using Equations (3).

The change in the state parameters of the GFCM concepts ("grayness" and "whiteness" of the state assessment) shown in Figures 3 and 4.

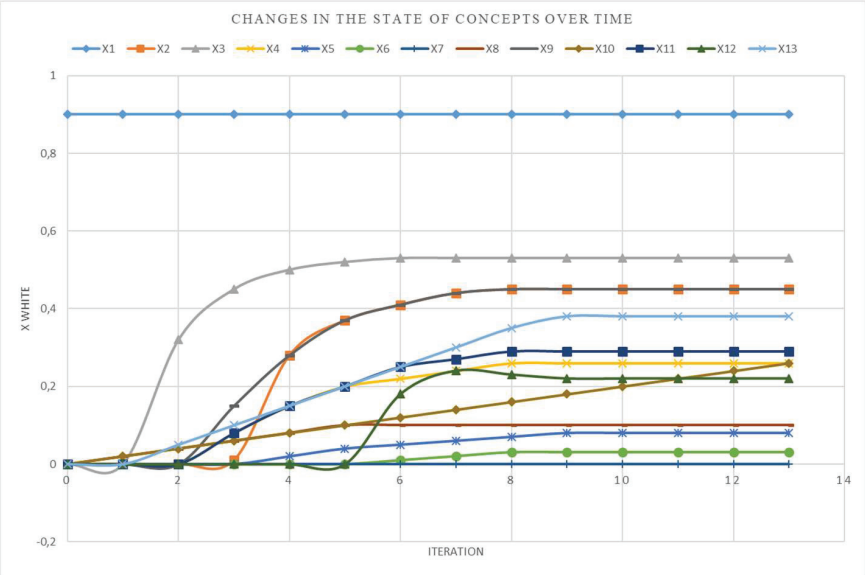

Figure 3 Temporal change of parameters of the state of GFCM concepts: stabilization of the "white" value of the concept.

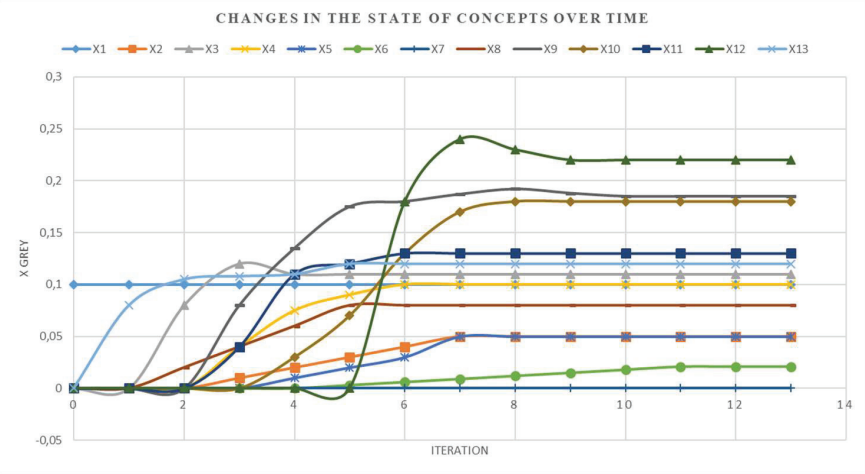

Figure 4 Temporal change of parameters of the state of GFCM concepts: stabilization of the "gray" concept.

4 Results & Discussion

Table 4 and Figure 5, which shows the results of modeling the operation of a printing company in the event of the occurrence of local relative risks and cyber security threats for the target concepts: C_5, C_7, C_{10}, C_{13}.

The local relative risk Ri means the potential damage caused to the i-th asset of the company's ICS (in relative units) and which leads to a violation of the integrity of telemetric information containing information about the balance of material flows at the facility and to a violation of the operation of the TP itself.

Note that the average assessment of local risks, which formed using an ensemble of cognitive maps, is better from the point of view of the dispersion of assessments of the state of the target concepts than the use of individual FCMs. The spread of estimates of the state of ensemble concepts is smaller than the spread of estimates of their gray values using GFCM, on average by

Table 4 Final results of modeling local risks and threats to cyber security of a printing enterprise

Type FCM	R_5	R_7	R_{10}	R_{13}
FCM	0,446	0,1	0,36	0,016
GFCM	0,463	0,11	0,36	0,025
R_i, GFCM	0,267	0,05	0,18	0,004
R_i, GFCM	0,7	0,17	0,530	0,044
Average value	0,454	0,105	0,36	0,0205

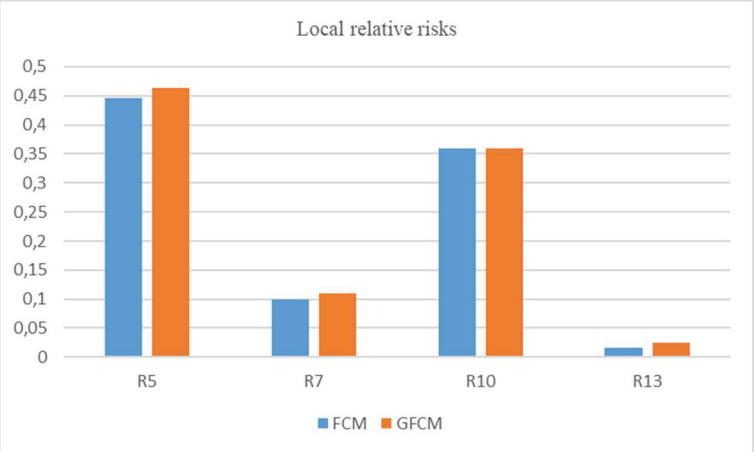

Figure 5 Local relative risks for selected target concepts.

1.4–1.8 times, which indicates a decrease in the influence of the subjectivity factor on the results of risk assessment.

As can be seen from Figure 5 constructed on the Table 4, the highest risk value corresponds to the target concept C5 (Unauthorized control of the printing station. Target concept (X5)), which in turn indicates the need to take additional measures to reduce this indicator. Carrying out it is possible, in particular, with the help of appropriate means of information protection: firewalls for industrial network segmentation, localization of network traffic within virtual networks, etc.

As the scenario modeling showed, the application of the specified means of protection and organizational measures allows reducing the assessment of local risks by 12–18%, which is a significant indicator.

Thus, application of the offered method of fuzzy cognitive design enables to provide the grounded high-quality and quantitative estimation of indexes of cyber security of the ISU of a printing enterprise taking into account opinions of experts – specialists of subject industry., that, in same queue, can become basis for the choice of effective measures of counteraction in accordance with the requirements of today's.

5 Conclusions

The study focuses on the logical-cognitive method of assessing the quality of minimizing the risks of information loss and illegal possession of data. In addition to the above, an order formation model built, which based on a modern cross-platform internet portal for the provision of printing services with a multidisciplinary flexible interface and the capabilities of dynamic data display and monitoring available in dispatching and control systems for printing processes.

The paper examines the use of classic and gray fuzzy cognitive maps to solve the problem of cyber security risk assessment of the intelligent management system of a printing enterprise. It demonstrated that the average estimate of local risk, which formed using an ensemble of two heterogeneous fuzzy cognitive maps, decreases compared to the use of individual cognitive maps. With the purpose of the best elucidation of research results, an example of the application of the proposed methodology for assessing the risks of ensuring the integrity of telemetric information in the industrial network of the intelligent technological process management system of a printing enterprise is given, with the continuity of the technological process of manufacturing printing products.

In addition to the classic FCM, the paradigms of two variants of the FCM extension used in the research, namely, the gray FCM, which used to solve the problem of assessing cyber security risks of intelligent management systems of printing enterprises. An analysis of the possibility of building FCM ensembles to increase the effectiveness of risk assessment using several options for formalizing the expert's knowledge and experience performed.

A fragment of the enterprise management system considered and an analysis of possible directions of attacks on the printing enterprise by malicious software performed. Basically, these attacks such as replacing the executable files of server and ARM software, overwriting PLC projects during system operation, and refusing to service the equipment.

Based on the formed list of attack vectors and the consequences of their implementation, the task of analyzing the risks of cyber security of a printing enterprise, taking into account the impact on the system of possible internal threats, was considered, using the cognitive modeling apparatus as a modeling tool.

The scenario of cognitive modeling of the influence of an internal criminal who exploits the vulnerabilities of the software and hardware components of the control system using the given variants of FCM construction is considered.

The average assessment of local risks, which formed using an ensemble of cognitive maps, is better from the point of view of dispersion of assessments of the state of target concepts than the use of individual FCMs. The spread of estimates of the state of ensemble concepts is smaller than the spread of estimates of their gray values using the GFCM, on average by 1.4–1.8 times, which indicates a decrease in the influence of the subjectivity factor on the results of risk assessment.

The performed scenario modeling showed that the use of the specified means of protection and organizational measures allows reducing the assessment of local risks by 12–18%, which is a significant indicator.

Thus, the proposed technique allows obtaining a qualitative and quantitative assessment of risk indicators, taking into account a set of objective and subjective factors of uncertainty.

References

[1] T. Liu, J. Tian, J. Wang et al., "Integrated security threats and defense of cyber-physical systems," Acta Automatica Sinica, vol. 45, no. 1, pp. 5–24, 2019.

[2] Ge Guo, W. Zhang, and B. Zhou, "Preface to the column "theory, method and application of cyber-physical system," Control and Decision, vol. 34, no. 11, pp. 2273–2276, 2019.
[3] Zahra, S. W., Arshad, A., Nadeem, M., Riaz, S., Dutta, A. K., Alzaid, Z., Almotairi, S. (2022). Development of security rules and mechanisms to protect data from assaults. Applied Sciences (Switzerland), 12(24) doi: 10.3390/app122412578.
[4] Sabat, V., Sikora, L., Durnyak, B., Fedevych, O., and Lysa, N. (2022). Information technologies of active control of complex hierarchical systems under threats and information attacks. Paper presented at the CEUR Workshop Proceedings, 3156, 305–318.
[5] Avsentev, O. S., Drovnikova, I. G., Zastrozhnov, I. I., Popov, A. D., and Rogozin, E. A. (2018). Control techniques of information resource protection of electronic document management system. SPIIRAS Proceedings, 2(57), 188–210. doi: 10.15622/sp.57.8.
[6] Sabat V. I., Matsyuk V. V., Musiyovska M. M., Kanevska N. I. 2020. Development of a system for managing access to documents in ASDO for printing publishers. Proceedings. No. 2 (60). pp. 68–74.
[7] Shepita P. I. 2019. Information model of a dynamic web service of an intelligent management system. Computer technologies of printing. No. 2 (42). pp. 73–80.
[8] Shepita P. I. 2018. Synthesis of an information model of intelligent management of printing production based on artificial neural networks. Modeling and information technologies. No. 85. pp. 192–196.
[9] Sabat V. I., Shepita P. I. 2018. Functional model of the protection system of the automated document management system. Modeling and information technologies. No. 84. pp. 190–195.
[10] Weng, M., and Weng, D. 2021. Discuss the Accounting Information Risks and Preventive Measures Based on Big Data. In 2021 2nd International Conference on Modern Education Management, Innovation and Entrepreneurship and Social Science (MEMIESS 2021) (pp. 110–114). Atlantis Press.
[11] Gao, J. 2022. Analysis of enterprise financial accounting information management from the perspective of big data. International Journal of Science and Research (IJSR), 11(5), 1272–1276.
[12] Imanbayev, A., Tynymbayev, S., Odarchenko, R., Gnatyuk, S., Berdibayev, R., Baikenov, A., and Kaniyeva, N. (2022). Research of machine learning algorithms for the development of intrusion detection

systems in 5G mobile networks and beyond. Sensors, 22(24) doi: 10.3 390/s22249957.

[13] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., and Marchetti, M. 2018. On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371–390). IEEE.

[14] Wickramasinghe, C. S., Marino, D. L., Amarasinghe, K., and Manic, M. 2018. Generalization of deep learning for cyber-physical system security: A survey. In IECON 2018 – 44th Annual Conference of the IEEE Industrial Electronics Society (pp. 745–751). IEEE.

[15] Tkachuk, R. L., Sikora, L. S., Lysa, N. K., Tupychak, L. L., Talanchuk, R. R., Fedyna, B. I., and Fedevich, Y. O. 2021. Information and cognitive technologies for assessing the situation in automated control systems under the influence of obstacles and failure factors. Computer technologies of printing. 2021. No. 1 (45). pp. 110–130.

[16] Fujs, D., Miheliè, A., and Vrhovec, S. L. 2019. The power of interpretation: Qualitative methods in cybersecurity research. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1–10).

[17] Torbacki, W. 2021. A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. Sustainability, 13(16), 8833.

[18] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., and Meskin, N. 2020. Cybersecurity for industrial control systems: A survey. Computers & security, 89, 101677.

[19] Stylios, C. D., Bourgani, E., and Georgopoulos, V. C. 2020. Impact and applications of fuzzy cognitive map methodologies. In Beyond traditional probabilistic data processing techniques: Interval, fuzzy etc. Methods and their applications (pp. 229–246). Springer, Cham.

[20] Osoba O.A., Kosko B. 2017. Fuzzy cognitive maps of public support for insurgency and terrorism // The Journal of Defense Modeling and Simulation. Vol. 14. No. 1. pp. 17–32. DOI: 10.1177/1548512916 680779.

[21] Salmeron, J. L., and Palos-Sanchez, P. R. 2019. Uncertainty propagation in fuzzy grey cognitive maps with hebbian-like learning algorithms. IEEE Transactions on Cybernetics, 49(1), 211–220. doi: 10.1109/TC YB.2017.2771387.

[22] Hajek, P., and Prochazka, O. 2016. Interval-valued fuzzy cognitive maps for supporting business decisions. Paper presented at the 2016

IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2016, 531–536. doi: 10.1109/FUZZ-IEEE.2016.7737732.

[23] Wang, J., Peng, Z., Wang, X., Li, C., and Wu, J. 2020. Deep fuzzy cognitive maps for interpretable multivariate time series prediction. IEEE transactions on fuzzy systems, 29(9), 2647–2660.

[24] Hajek, P., Froelich, W., and Prochazka, O. 2020. Intuitionistic fuzzy grey cognitive maps for forecasting interval-valued time series. Neurocomputing, 400, 173–185. doi: 10.1016/j.neucom.2020.03.013.

[25] Salmeron, J. L. 2015. A fuzzy grey cognitive maps-based intelligent security system. Paper presented at the Proceedings of IEEE International Conference on Grey Systems and Intelligent Services, GSIS, 2015-October 29–32. doi: 10.1109/GSIS.2015.7301813.

[26] Lei, Y., Kong, W., and Ma, J. 2017. Intrusion detection techniques based on improved intuitionistic fuzzy neural networks. International Journal of Innovative Computing and Applications, 8(1), 41–49. doi: 10.1504/IJ ICA.2017.082496.

[27] Reji, M., Kishore Raja, P. C., Joseph, C., and Baskar, R. 2017. A genetic-fuzzy approach for detection of worm attack in ad-hoc wireless networks. Indian Journal of Public Health Research and Development, 8(4), 1312–1321. doi: 10.5958/0976-5506.2017.00517.4.

[28] Durnyak, B., Lutskiv, M., Shepita, P., and Nechepurenko, V. 2020. Simulation of a combined robust system with a P-fuzzy controller doi: 10.1007/978-3-030-26474-1_39.

[29] Durnyak, B., Lutskiv, M., Petriaszwili, G., and Shepita, P. 2020. Analysis of raster imprints parameters on the basis of models and experimental research. Paper presented at the International Symposium on Graphic Engineering and Design, 379–385. doi: 10.24867/GRID-2020-p42.

[30] Nguyen, D. H., de Leeuw, S., and Dullaert, W. E. 2018. Consumer behaviour and order fulfilment in online retailing: A systematic review. International Journal of Management Reviews, 20(2), 255–276.

[31] Sengupta, J., Ruj, S., and Bit, S. D. 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481.

[32] Ghobakhloo, M. 2020. Industry 4.0, digitization, and opportunities for sustainability. Journal of cleaner production, 252, 119869.

[33] Deng, L., Sun, H., and Li, C. 2021. JDF-DE: a differential evolution with Jrand number decreasing mechanism and feedback guide technique for global numerical optimization. Applied Intelligence, 51(1), 359–376.

[34] Hoffmann-Walbeck, T. 2018. Smart factory: JDF and XJDF. J. Graph. Eng. Des, 9(1), 5–9.
[35] Faraj, B.M. and Ahmed, F.W., 2019. On the matlab technique by using laplace transform for solving second order ode with initial conditions exactly. Matrix Science Mathematic, 3(2), pp. 08–10.
[36] Jaafar, S.S. and Mahmood, F.M., 2020. Design and Programming of a Micro-controller-Based Solar Tracking System.
[37] Faraj, B. and Mondali, M., 2017. Using difference scheme method for the numerical solution of telegraph partial differential equation. Journal of Garmian University, 4(ICBS Conference), pp. 157–163.

Biographies

Petro Shepita received a bachelor's degree in 2016 and a master's degree in 2018 at the Ukrainian Academy of Printing (Ukraine). Received the degree of Doctor of Philosophy in the specialty "information systems and technologies" in 2021 at the Ukrainian Academy of Printing (Ukraine). Senior lecturer of the Department of Computer Sciences and Information Technologies of the Ukrainian Academy of Printing. Field of scientific interests: intelligent management systems, IoT (IIoT), decision support systems, cyber security of intelligent systems.

Lyubov Tupychak Graduated from the Ukrainian Academy of Typography with a major in "Publishing and editing". Defended the dissertation work "Information technologies for supporting management decisions in the educational process using logical-cognitive methods" to obtain the scientific degree of Candidate of Technical Sciences in the major "Information Technologies". Scientific interests: Informational and cognitive concepts of processes of intellectual activity of a person during decision-making in crisis conditions; development of information technologies to support management decisions in the educational process using logical-cognitive methods to improve the quality of the educational process and the level of competence of specialists.

Julia Shepita received a bachelor's degree in 2022, is getting a master's degree in computer science at the Ukrainian Academy of Printing (Ukraine). Scientific interests: cyber security of intelligent control systems.