Protection of the Information System of the Printing Enterprise from Cyber Threats

Bohdan Durnyak[a], Petro Shepita[a] , Lyubov Tupychak[a]

[a] *Ukrainian Academy of Printing, Pid Goloskom str., 19, Lviv, 79020, Ukraine*

Abstract

The article considers the challenges of cybersecurity that appear at the current stage of information technology development, along with the introduction of artificial intelligence and machine learning. Based on the generated information about the production processes and ways of filling in the knowledge base and the database, a model for creating a knowledge base and expert simulation developed, which made it possible to make an optimal assessment of expert knowledge, and in the event of their contradiction, use the knowledge of the simulated expert. Protection against attacks by competitors provided with the replacement of correct information. Modeling of the system's operation under the conditions of a competitive FGM attack carried out. Analysis of the transient characteristics showed that as the epsilon index increases, distortion of the samples occurs, leading to the loss of data important for the operation of the system. In turn, the number of copies for which a decision made decreases, and thus the accuracy of recognizing error signals and disturbances obtained during the operation of printing devices partially reduced. Considering that, the samples that have not passed the inspection not admitted to the decision-making stage on them and do not affect the accuracy. The system works in normal mode and minimizes or even eliminates the influence of competition, depending on the epsilon, designed the printing house management system, thanks to a simulated expert and protection against competition attacks, will ensure the continuity of the production plant processes. Experiments carried out that show the effectiveness of the development in both increasing the accuracy of the classifier and ensuring its reliable operation in the conditions of a competitive attack.

Keywords 1

Printing company, Internet of things, artificial neural network, cyber-attack, knowledge base

1. Problem Setting

The introduction into the technological process of small printing houses of existing control and data collection systems with a relatively significant cost of highly specialized equipment, mainly built-in equipment with a limited range, the need to arrange dispatch and server rooms, access to individual workstations, requires highly qualified operators and valuable maintenance, which significantly increases and services provided. The problem of the use of information technologies in printing focused on the study of materials and devices, the analysis of individual effects on the quality of printing, rasterization methods and their impact on image color transfer, on the development of automation and measures for the informatization of printed products. In the conditions of innovative reform, the company has a growing need to design technologies for optimizing and managing multi-stage information processes, in particular machine and device construction, in the printing industry, and in education informatization systems. Today, either the list of industries, which the operator makes, decisions at key stages of the technological process or when coordinating the stages between

IntelITSIS'2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine

EMAIL: durnyak@uad.lviv.ua (B.Durnyak); pshepita@gmail.com (P. Shepita); ltupychak@gmail.com (L. Tupychak);

ORCID: 0000-0003-1526-9005 (B. Durnyak); 0000-0001-8134-8014 (P. Shepita); 0000-0002-0963-3360 (L. Tupychak);

them of the technological process is expanding. Significant progress in the modernization of the enterprise achieved through the introduction of production complexes, which integrated into the existing technological process with the gradual elimination of the outdated elementary base in the weakest places, in particular, which will allow the analysis of production resources in order to make an appropriate management decision. Along with the implementation of such necessary and modern information technologies, there are several threats associated with cyber security. Overall, the development of machine learning and artificial intelligence not only facilitated the mental activity of users in Internet of Things or Industrial Internet of Things, but also created an environment for growth. The most common reason is the breakdown of the machine-learning model. An adversarial attack can consist of presenting a model with inadequate or fake data during training, or injecting maliciously crafted data to fool an already trained model. There is therefore an urgent need to explore the protection of information systems with elements of artificial intelligence implemented in printing enterprises.

Therefore, there is an urgent need to take into account the existing threats to information management systems when informatizing the work of a printing company and to prevent their penetration into the system at the design stage.

2. Analysis of recent research and publications

One of the important sources about the lack of protection of artificial intelligence systems considered the report of the US National Security Commission [1], which refers to a very small number of studies specifically devoted to the protection of artificial intelligence systems. In addition, disregarding basic cybersecurity rules for conducting scientific research. In addition, some systems already deployed in production are also not 100% protected against attacks. In the article [2], the authors placed an improvised road marking on the surface of which a car with autopilot moves, which caused the car to leave the oncoming lane. In [3], it shown that small and almost imperceptible changes in the selections intended for medical diagnostics could lead to a targeted diagnosis and cause harm to a person. The authors of the research [4] gave an example of how a road sign learned by a car control system with machine learning can easily lead to an accident by correcting it with improvised means. In the article [5, 6, 7], scientists from Google and the University of California proved that even the best forensic classifiers - artificial intelligence systems developed by the US Departments of State Security, taught to distinguish and separate real and synthetic content under attack. As noted by [8-12] VentureBeat participants, there has been a surge in research on competitive attacks in recent years. Therefore, from 2014 to 2022, on the Arxiv.org preprint server, the number of articles submitted on competitive machine learning increased from two to about 1,800, while in 2020, there are about 1,000 articles on competitive samples and attacks. Competing attacks on artificial intelligence systems have received wide coverage at the international conferences ICLR, Usenix and Black Hat. Therefore, when designing and developing systems for IIoT, it is necessary to ensure protection against attacks by competitors.

3. Presentation of the main research material

The article treats the management of a printing company as an integral structure based on elements of artificial intelligence and machine learning. Using the available elements of information technology, a decision-making system built based on the training of an artificial neural network and the creation of a knowledge bank. Two implementation variants are considered and an analysis of the system's response to external threats carried out.

The scientific novelty of the presented research consists in the development of a model for the formation of a knowledge base and imitation of an expert with the help of physical experts and the apparatus of artificial neural networks.

3.1. Building an expert simulator and training ANNs by conventional means

In the classic presented to ensure the functioning of the management system, a knowledge base is used in the formation of which experts participate, the number of which depends both on the need and on the availability of experts in the given field and technologies, this method is typical for expert systems, supervisory management systems. However, the knowledge base is quite subjective and has a human factor influencing the formation of records. In order to increase the efficiency of the intelligent management system, it proposed to implement the knowledge bank and expand the sources of its content [13-18].

When building an intelligent management system for a printing enterprise, which performs complex order support, a set of tools used, which organizes the interaction of the executive system and a set of intelligent interface tools, which have a flexible structure and provide the possibility of adaptation in a wide range of end-user interests. A knowledge bank serves as such a means, which ensures the use of basic complexes of a complete and independent from third-party programs system of knowledge about the environment by means of computing [19, 20].

The knowledge bank occupies a central place in relation to the rest of the components of the management system. Its formation consists of developed behavior management systems and has a number of information inputs and management outputs. For this purpose, the following options for forming a knowledge bank considered (Fig. 1).

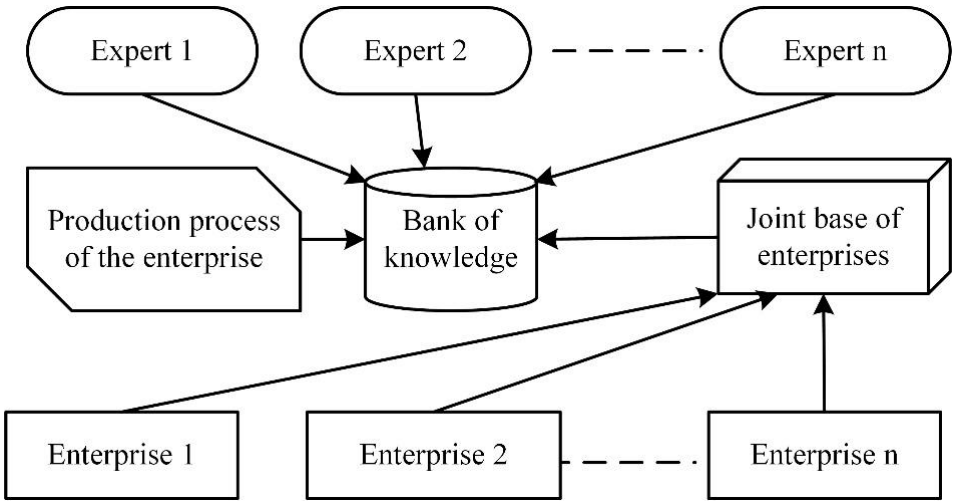

Figure 1: Collection of information for the formation of a knowledge bank of an intelligent management system

The first stage is to fill the knowledge base with expert knowledge, which allows you to start the operation of the ICS without the main units of equipment working. More time-consuming, but more effective for a specific enterprise, is the stage of forming the DB based on the production data of the equipment available at the enterprise. For this purpose, constant monitoring of management objects carried out, when failures detected in the process of performing a production task, management actions on the object recorded and an assessment of the quality of elimination of deficiencies and failures in the process carried out. On the basis such data, a structural unit of the knowledge bank is formed - the corporate base of the enterprise [21, 22]. For the implementation of the third stage of BnZ filling, the optimal solution was the use of cloud technologies, which allow combining corporate databases into centralized one [23]. Where tables formed in accordance with the type of equipment used at one or another enterprise. In this way, the training sample increases and becomes more flexible, since different units of the same equipment have their own characteristics of work, in this regard, deviations in work may appear at different times, depending on the materials used, the load on the units, etc.

At the same time, enterprises can communicate with each other, improving their management systems and increasing their efficiency and autonomy. Thus, when using cloud technologies to create a knowledge bank of ICS, a large and diverse sample formed, which allows for the creation of a flexible analytical apparatus of the management system [24-26].

On the basis of the obtained stages of formation of the knowledge bank, the construction of the model of the functioning of the control system elements with the established flows of the production cycle of order manufacturing was performed (Fig.2). The analytical apparatus of the ICS performs control functions over the production process, along with this; it interacts with the knowledge bank, which expands its capabilities by eliminating the shortcomings of the equipment that affect the quality of products [27].

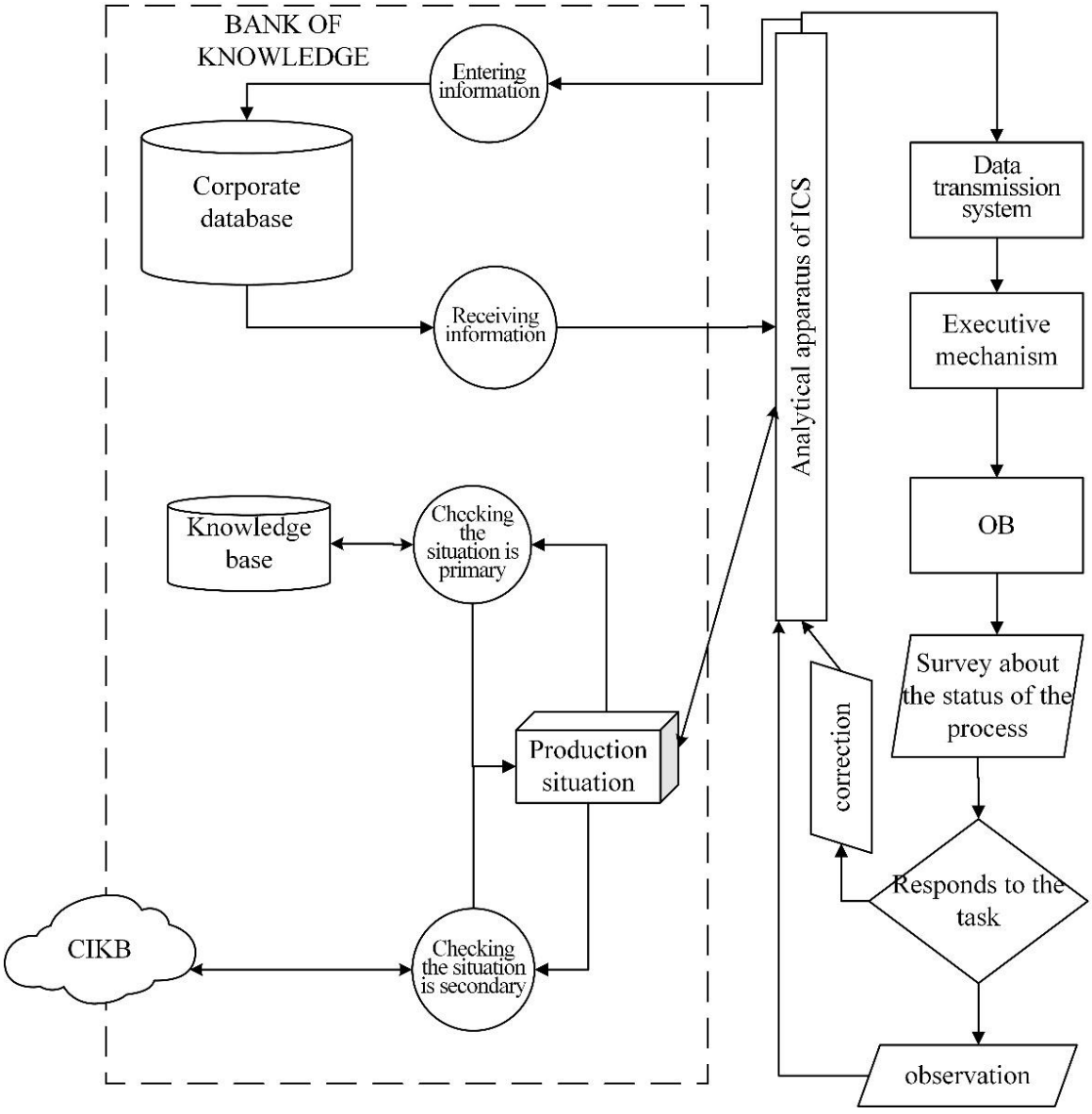

Figure 2: Model of interaction of elements of the control system with knowledge flows

When considering the production situation, the company's knowledge base serves as the primary source of knowledge about the process, on its basis, the behavior of the management system formed during the elimination of disturbances and the adjustment of production processes. In order to build a behavior management system that meets all the listed requirements, it is necessary to resolve the issue of organizing the knowledge base of such a system and its mechanism of logical conclusion [28].

The structure of the knowledge base of the management system of a multi-level complex proposed organized according to the stages depicted in fig. 3.

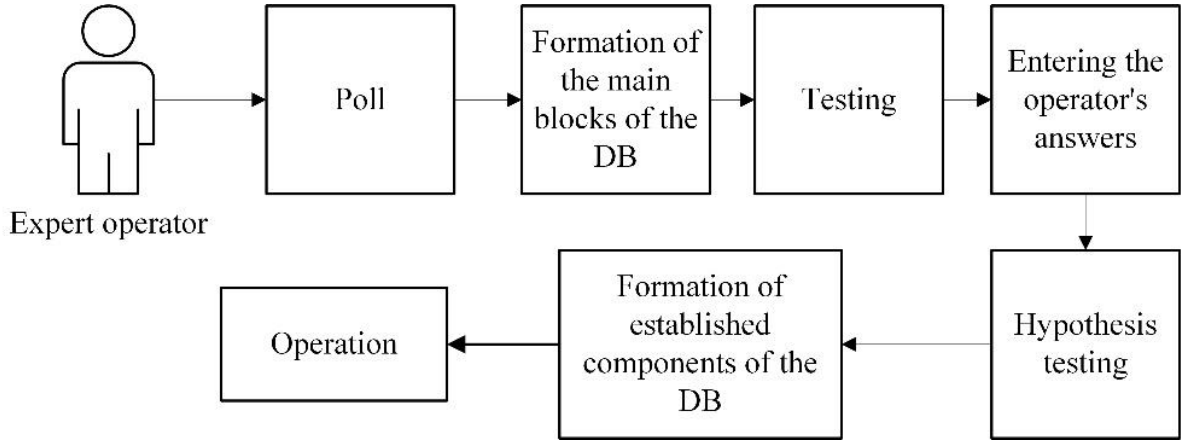

Figure 3: Stages of formation of the ICS knowledge base

The main element of the enterprise management system is the analytical unit, which is responsible for understanding the problem and solving tasks as well as locating faults. First, the parameters and main blocks of the knowledge base created. An operator-expert survey carried out, in which the main stages and important points of operation of technological devices defined (Fig. 1). Since the existing knowledge base also used at the stages preceding the direct production of products, the study also carried out among other experts.

In order to create a knowledge base, a production goal is defined, after which a number of expert operators (Fig. 4) OEn are interviewed, who describe the situation St occurring in the work process, and also describe the control of the Kv action that must be performed to achieve the required result Rz. These data are the characteristics of the experts:

$$OE_n = \{St, Kv, Rz\} \quad (1)$$

In order to normalize the presentation of survey information for each of the expert operators, the following mathematical relationship created:

$$St_n + Kv_n = Rz_n \quad (2)$$

where the numerical values obtained when testing expert operators received as input, which in turn is equal to the resulting value of the control action.

A comparison is made of the results obtained as result of mathematical operations:

$$G_n = |Rz_n - Rz_{n+1}| \quad (3)$$

where G is the difference between the resulting scores of expert operators;

The parameter G obtained by the formula (3) is included in the unit of creating the knowledge competence value in which the mathematical operation summation carried out:

$$FVK = \sum_{i=1}^{n} G_i \quad (4)$$

If the knowledge value of the competences obtained as result of mathematical operations is less than 0.5n, the corresponding entry in the knowledge base created and marked as correct. If the specified condition not met, i.e. "false", then these claims will be marked as untrustworthy. In this context, an expert simulation block introduced into the model. In order to obtain the expected result based on the obtained statements of expert operators, after analyzing the used algorithms that would meet the needs of the system, the optimal variant of the use of artificial neural networks (ANN) selected. Then, a dataset of objects is created in the form of a training sample for an artificial neural network from the data obtained from experts to produce 1 [29-31].

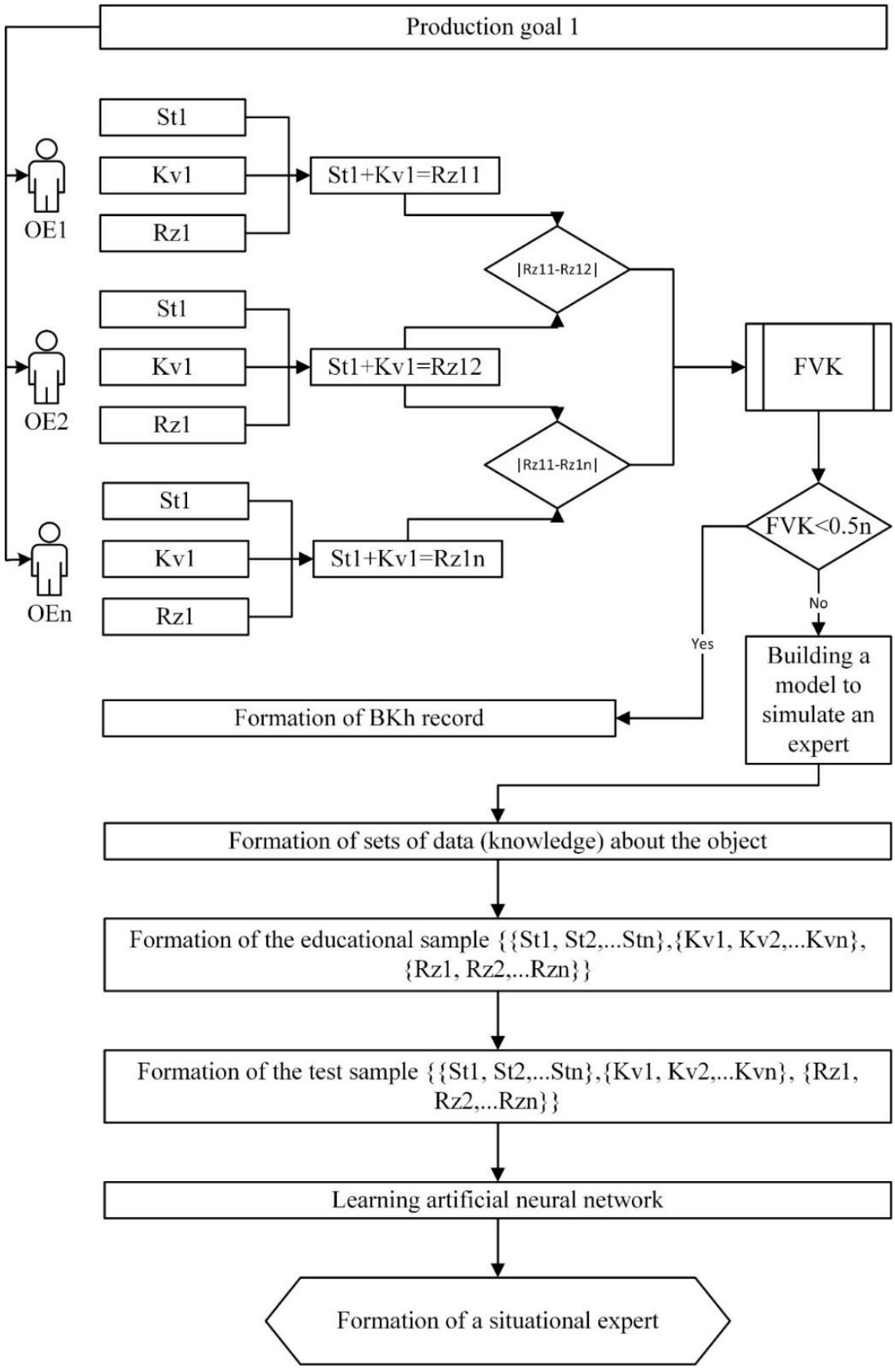

Figure 4: A model of knowledge base formation and imitation of an expert

For the implementation of the above situational expert, a neural network with forward propagation and the fastest descent method, which implemented using the Levenberg-Marquardt algorithm. The training sample created from normalized data for a selected production situation, which obtained during a survey of expert operators. The created input value vector, which consists of expert opinions, fed to the input of the neural network. This vector obtained during the test reflects the parameters that are necessary to train the IT system and its further functioning.

$$X = [St_1] \tag{5}$$

After processing the data using the normalization algorithm, a vector of values created at the output of the artificial neural network, which we treat as initial data:

$$Y = \begin{bmatrix} Rz_1 \\ Kv_1 \end{bmatrix} \tag{6}$$

To formalize the representation, we treat the neural network as the expression of its output Y=Y(X, Q) after performing the functions correcting the weighting factors of neurons Q.

An expression (7) used to calculate the neural network error for one epoch:

$$F(Y) = \frac{1}{2}((St_1 - Rz_1)^2 + (Kv_1 - Rz_1)^2) \tag{7}$$

Since the Levenberg-Marquardt algorithm chosen, the training input sample divided as follows. The largest number of examples is needed to train the network, so 70% of the total data is allocated to it, the other two subsamples do not require a large number of examples, so each of the samples used will receive 15% of the records from the entire sample for verification and research [9, 17, 36, 37].

3.2. Learning ANNs for recognition from adversarial attacks

The necessary normalized data has been imported to start training and running the neural network. After a successful import, the CNN built and trained using pure data without any additional training data. In order to avoid possible external interference in the operation of the enterprise management system, the construction of the TrustScore auto encoder model and its training on the existing data set implemented. The purpose of the performed operations is to calculate the parameters of trust in the company's knowledge base and the set of data used in training. First, all training data is preprocessed to find a high density α sample from each class defined as training samples in the selected class after filtering out the α fraction of the samples with the lowest data density.

Let $0 \leq \alpha < 1$ and f be a continuous density function with a compact support $X \subseteq RD$. On the mastering of the announced information, it is determined $H\alpha(f)$, an α-set f which has a high data density, is identical to the set of level $\lambda\alpha\, f$ defined as a mathematical dependence:

$$\{x \epsilon X: f(x) \geq \lambda\alpha\}\, where\ \lambda\alpha \coloneqq inf\{\lambda \geq 0: \int X_1[f(x) \leq \lambda] f(x)dx \geq \alpha\} \tag{8}$$

To perform the operation of approximation of the α-high density data set, filtering of the α part of the points with the lowest empirical density was carried out on the basis of k-nearest neighbors data. The performed data-filtering step does not depend on the received classifier h. The next step was to provide a test sample for which the confidence score was determined as the ratio of linguistic data from the tested sample to the high-density α set of the nearest class, which is the opposite of the expected class. It assumed that if in the classifier h there is a label much further than the nearest label, and then based on such data a warning issued about possible unreliable statements of the simulated expert. Thus, the performed procedure can treated as a procedure of comparing the nearest neighbor with a modified classifier, in which the modification itself consists in the initial filtering of linguistic variables that do not belong to the high-density set α of each class.

To approximate the set of α-high density, the smallest empirical density, based on k-nearest neighbors, filters the α-fraction of points. This data-filtering step is independent of the given classifier h. The next stage is to provide a test sample; we determine the confidence estimate as the ratio between the linguistic data from the sample under study and the high-density α-set of the closest class, different from the predicted class. It assumed that if the classifier h predicts a label that is significantly further than the closest label, then this is a warning that the simulated expert may be wrong. Thus, our procedure can be seen as a comparison with a modified nearest neighbor classifier, where the modification is to initially filter out linguistic variables that are not included in the high-density α-set for each class.

3.3. Comparison of system performance

In the process of testing the traditional model and the autoencoder with TrusctScore on clean data and using disturbed samples with different disturbance values, the following results obtained, which shown in Fig. 5 and 6. The obtained characteristics indicate that the developed expert model of imitation characterized by significantly higher recognition accuracy and high resistance to adversarial FGM attacks compared to the traditional model characterizes it. However, even though the system has a fairly high performance, in the presence of strong high-epsilon disturbances, the data is heavily corrupted, which makes it actually unreliable, but even in this case, we can observe that the obtained accuracy, which is the basis of the agreement with TsustScore, is adequately higher.

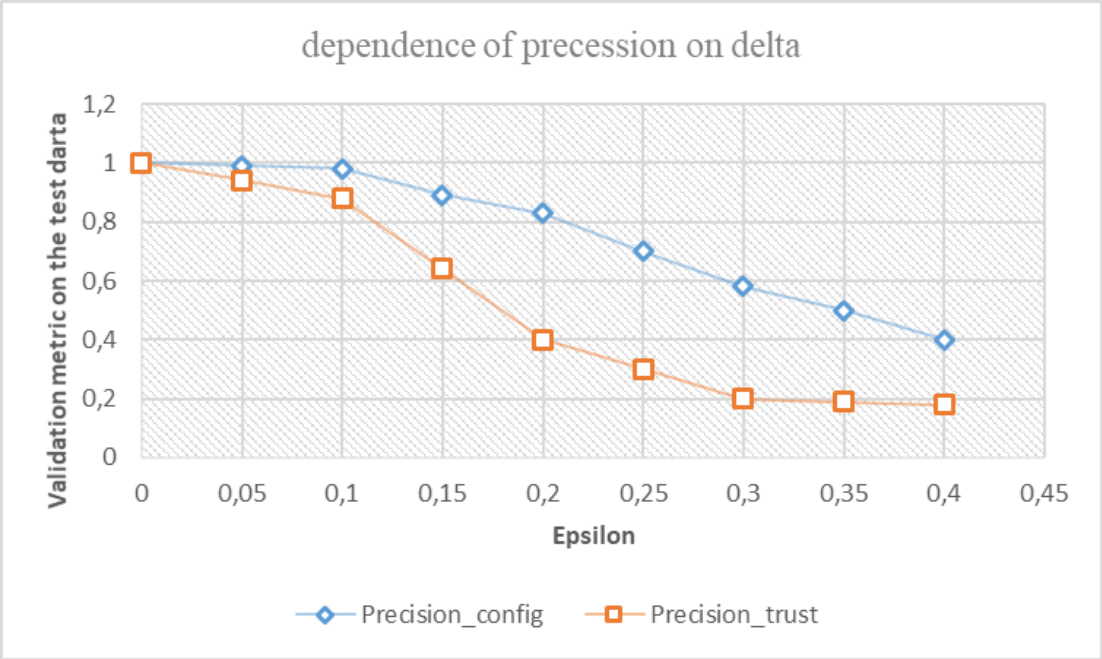

Figure 5: The dependence of precession on epsilon, where precision_config is the accuracy based on confidence at the output of a traditional classifier without an available corrector and has the form of trustscore; precision_trust – accuracy based on trustscore

An analysis of the obtained graphs was performed, which demonstrates that the accuracy of the classification in agreement with the trust score (Precision_trust) is significantly higher than the accuracy of the base classifier at all delta values, even when the considered samples contain external disturbance or(and) are strongly distorted.

The obtained transient characteristics analyzed. It becomes obvious that as the epsilon index increases, the samples are distorted, leading to the loss of important data for the operation of the system.

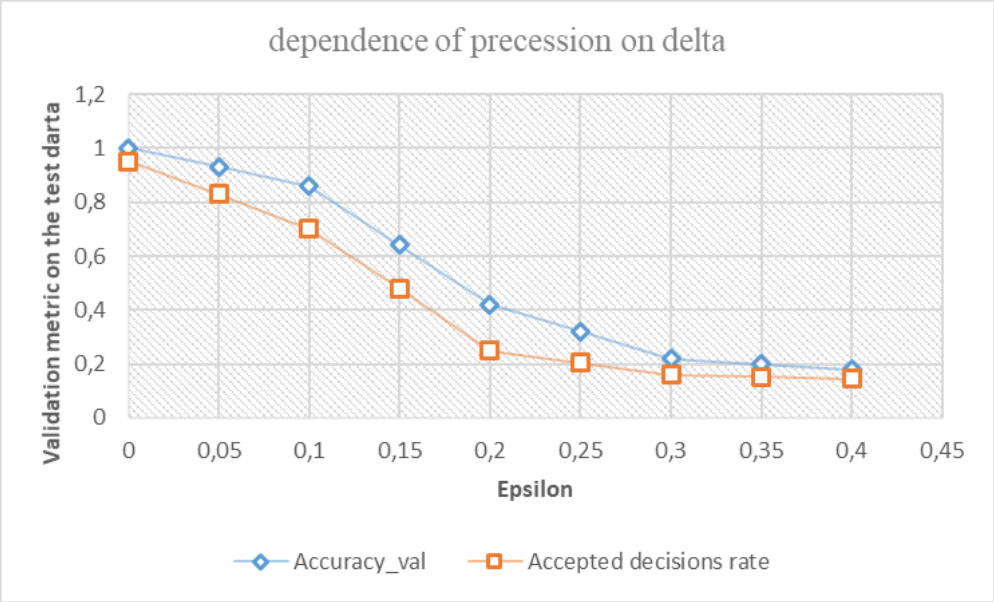

Figure 6: dependence of precession on delta, where Accuracy valuation is the classical accuracy of the basic classifier without adding a corrector presented in the form of trustscore.

In turn, the number of copies for which a decision made decreases, and thus the accuracy of recognizing error signals and disturbances obtained during the operation of printing devices partially reduced. Given that, samples that fail the test are not eligible for the decision-making stage and do not affect the accuracy of the production job inspection process. Whether the sample compromised or otherwise distorted, the system processes and minimizes or eliminates the impact of competition, depending on epsilon.

Thus, the designed management system for a printing company, thanks to a simulated expert and protection against attacks by competitors, will ensure the continuity of the production hall processes.

4. Conclusion

Artificial intelligence systems and Industrial Internet of Things tools, like any software tool, require protection against unauthorized access from the outside, reliability and safe operation in all respects and in all conditions. In accordance with the designated stages, the construction of the corporate knowledge bank of the printing company to store information on managing the order life cycle was completed. A model of interaction of management system elements with knowledge flows built in order to expand the operational knowledge bank and flexible access to the collected information. In order to train the analytical apparatus, a scenario of creating a knowledge base was developed, in which, in addition to the classic method of interviewing experts in a given field, knowledge gathered on the basis of monitoring processes and devices was added, which made it possible to develop a mathematical model of shaping the value of knowledge competencies.

Based on the generated information about the production processes and ways of filling in the knowledge base and the database, a model for creating a knowledge base and expert simulation developed, which made it possible to make an optimal assessment of expert knowledge, and in the event of their contradiction, use the knowledge of the simulated expert. Since the modern development of enterprises is associated with round-the-clock communication with the Internet, and the elements of the intelligent control system based on artificial neural networks, protection against competition attacks provided by replacing correct information. Modeling of the system's operation under the conditions of a competitive FGM attack carried out. After analyzing the obtained transient characteristics, it became obvious that with the increase of the epsilon index, the samples are distorted, which leads to the loss of data important for the operation of the system.

In turn, the number of copies for which a decision made decreases, and thus the accuracy of recognizing error signals and disturbances obtained during the operation of printing devices partially

reduced. Whereas unverified samples are non-decisive and do not affect the accuracy of the production job inspection process, whether or not the sample compromised or distorted for other reasons, the system processes and minimizes or even eliminates the impact of competition, depending on epsilon. The designed printing house management system will ensure the continuity of the production plant processes thanks to a simulated expert and protection against attacks by competitors.

As result of the conducted research, modern and effective technologies and approaches to the implementation of the analytical block of the printing company management system with the ability to recognize various types of cyberattacks on artificial intelligence systems and protect against them considered and analyzed. Experiments carried out that showed the effectiveness of the development both in terms of increasing the accuracy of the classifier, and in terms of ensuring its reliable operation in the conditions of a competitive attack.

5. References

[1] E. Schmidt, National security commissionon artificial intelligence interim report November 2019, National security commissionon artificial intelligence , Washington, 2019.

[2] Tencent Keen Security Lab. (2019, March). Experimental Security Research of Tesla Autopilot. Shenzhen, Guangdong, China; Tencent Keen Security Lab.

[3] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, I. S. Kohane, Adversarial attacks on medical machine learning. Science, 363 6433 (2019) 1287–1289. doi:https://doi.org/10.1126/science.aaw4399

[4] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song Robust physical-world attacks on Deep Learning Visual Classification. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018. doi: https://doi.org/10.1109/cvpr.2018.00175

[5] N. Carlini, H. Farid, Evading deepfake-image detectors with white- and black-box attacks. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). doi: https://doi.org/10.1109/cvprw50498.2020.00337

[6] Y.Zhu, Y.Jiang, Z.Peng, W. Huang, Fast category-hidden adversarial attack against Semantic Image segmentation. International Journal of Computational Intelligence Systems, 14(1), (2021) 1823. doi: https://doi.org/10.2991/ijcis.d.210620.002

[7] J. Wang, J. Liang, L. Zhang, X. Ding, Non-fragile dynamic output-feedback control for -gain performance of Positive FM-II model with PDT switching: An event-triggered mechanism. International Journal of Robust and Nonlinear Control, 32(6) (2022) 3986–4007. doi:https://doi.org/10.1002/rnc.6003

[8] I. O. Lopes, D. Zou, I.H. Abdulqadder, F.A. Ruambo, B. Yuan, H. Jin, Effective network intrusion detection via representation learning: A denoising AutoEncoder approach. Computer Communications, 194 (2022) 55–65. https://doi.org/10.1016/j.comcom.2022.07.027

[9] Y. Pan, P. Du, H. Xue, H.-K. Lam, Singularity-free fixed-time fuzzy control for robotic systems with user-defined performance. IEEE Transactions on Fuzzy Systems, 29(8) (2021) 2388–2398. doi:https://doi.org/10.1109/tfuzz.2020.2999746.

[10] A.-M. Creţu, F. Monti, S. Marrone, X. Dong, M. Bronstein, Y.-A. de Montjoye, Interaction data are identifiable even across long periods of time. Nature Communications, 13(1) (2022) doi:https://doi.org/10.1038/s41467-021-27714-6.

[11] B. Durnyak, M. Lutskiv, P. Shepita, V. Nechepurenko, Simulation of a Combined Robust System with a P-Fuzzy Controller. Intellectual Systems of Decision Making and Problems of Computational Intelligence: Proceedings of the XV International Scientific Conference, 1020, 2019 pp. 570-580.

[12] B. Imamović, S.S. Halilčević, P. S. Georgilakis, Comprehensive fuzzy logic coefficient of performance of absorption cooling system. Expert Systems with Applications, 190 (2022) 116185. doi:https://doi.org/10.1016/j.eswa.2021.116185

[13] A. A. Salem, A. A. ElDesouky, A.H. Alaboudy, New Analytical Assessment for fast and complete pre-fault restoration of grid-connected fswts with fuzzy-logic pitch-Angle Controller.

International Journal of Electrical Power & Energy Systems, 136 (2022) 107745. doi:https://doi.org/10.1016/j.ijepes.2021.107745
[14] P.Tang, Y. Ma, Exponential stabilization and non-fragile sampled-date dissipative control for uncertain time-varying delay T-s fuzzy systems with state quantization. Information Sciences, 545 (2021) 513–536. doi: https://doi.org/10.1016/j.ins.2020.09.036
[15] J. Lin, , L. L. Njilla, , K. Xiong, Secure machine learning against adversarial samples at Test Time. EURASIP Journal on Information Security, 2022(1). doi: https://doi.org/10.1186/s13635-021-00125-2.
[16] M. J.Mahmoodabadi, M. Andalib Sahnehsaraei, Parametric uncertainty handling of under-actuated nonlinear systems using an online optimal input–output feedback linearization controller. Systems Science & Control Engineering, 9(1) (2021) 209–218. doi:https://doi.org/10.1080/21642583.2021.1891993
[17] J. Yoo, D. Lee, C. Son, S. Jung, B.I. Yoo, C. Choi, J.-J. Han, B. Han, Rascanet: Learning tiny models by raster-scanning images. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). doi: https://doi.org/10.1109/cvpr46437.2021.01346
[18] B. Durnyak, M. Lutskiv, P. Shepita, R. Karpyn, N. Savina, Determination of the Optical Density of Two-Parameter Tone Transfer for a Short Printing System of the Sixth Dimension. Paper presented at the CEUR Workshop Proceedings, 2853, (2021) 34-140
[19] Z. Li, K. Xu, H. Wang, Y. Zhao, X. Wang, M. Shen, M. Machine-learning-based positioning: A survey and Future Directions. IEEE Network, 33(3) (2019) 96–101. https://doi.org/10.1109/mnet.2019.1800366
[20] M. Ibrahim, A. Hadiwibowo, M. Djaiz, H.N. Sukma, DGM 430 offset web Machine Print Quality. KREATOR, 2(2) (2021). https://doi.org/10.46961/kreator.v2i2.287
[21] Jaiswal, E., Globisch, C., & Jain, A. (2022). Knowledge-driven design and optimization of potent symmetric anticancer molecules: A case study on PKM2 activators. Computers in Biology and Medicine, 151, 106313. https://doi.org/10.1016/j.compbiomed.2022.106313
[22] J. Zhao, Z. Chen, J. Tu, Y. Zhao, Y. Dong, Application of LSTM approach for predicting the fission swelling behavior within a cercer composite fuel. Energies, 15(23) (2022) 9053. https://doi.org/10.3390/en15239053
[23] J.Canada-Bago, J.-A. Fernandez-Prieto, A knowledge-based battery controller for IOT Devices. Journal of Sensor and Actuator Networks, 11(4) (2022) 76. https://doi.org/10.3390/jsan11040076
[24] F. Long, L. Ding, J. Li, DGFlow-Slam: A novel dynamic environment RGB-D slam without prior semantic knowledge based on grid segmentation of scene flow. Biomimetics, 7(4), (2022) 163. doi: https://doi.org/10.3390/biomimetics7040163
[25] J. Peng, G. Xia, Y. Li, Y. Song, M. Hao, Knowledge-based prognostics and health management of a pumping system under the linguistic decision-making context. Expert Systems with Applications, 209 (2022) 118379. doi: https://doi.org/10.1016/j.eswa.2022.118379
[26] V. T. Nguyen, N. T. Nguyen, T. H. Tran,. Knowledge integration methods for probabilistic knowledge-based systems, 2022. doi: https://doi.org/10.1201/9781003277019
[27] B. Durnyak, M. Lutskiv, P. Shepita, V. Sheketa, R. Karpyn, N. Pasyeka, Analysis of transfer of modulated ink flows in a short printing system of parallel structure. Advances in Computer Science for Engineering and Education, (2022) 17–26. doi: https://doi.org/10.1007/978-3-031-04812-8_2
[28] B. Durnyak, M. Lutskiv, G. Petriaszwili, P. Shepita, Analysis of raster imprints parameters on the basis of models and experimental research. Proceedings - The Tenth International Symposium GRID 2020. doi: https://doi.org/10.24867/grid-2020-p42
[29] B. Durnyak, M. Lutskiv, P. Shepita, R. Karpyn, V. Sheketa, M. Pasieka, Modelling of tone reproduction with round raster elements in a short printing system of parallel structure. Advances in Computer Science for Engineering and Education, (2022) 37–46. doi:https://doi.org/10.1007/978-3-031-04812-8_4
[30] D. Attique, H. Wang, P.Wang, Fog-assisted deep-learning-empowered intrusion detection system for RPL-based resource-constrained smart industries. Sensors, 22(23), (2022) 9416. doi:https://doi.org/10.3390/s22239416