Journal of Theoretical and Applied Information Technology
15th June 2023. Vol.101. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BUILDING A NEURAL NETWORK TO ASSESS THE LEVEL OF OPERATIONAL RISKS OF A CREDIT INSTITUTION

EKATERINA VITALEVNA CHUMAKOVA[1], DMITRY GENNADIEVICH KORNEEV[2], MIKHAIL SAMUILOVICH GASPARIAN[3], ANDREY ALEKSANDROVICH PONOMAREV[4], ILIA SERGEEVICH MAKHOV[5]

[1]Moscow Aviation Institute, MAI, 4 Volokolamskoe shosse, Moscow, 125993, Russia

[2,3,4,5]Plekhanov Russian University of Economics, 36 Stremyanny lane, Moscow, 117997, Russia

E-mail: m.sam.gasparian@gmail.com

ABSTRACT

This article considers the issues of managing the operational risks of a credit institution arising in the process of using information technologies. To manage operational risks associated with the use of IT in banks, the authors propose methods based on the use of artificial neural networks. The decisive stage in operational risk management is the collection and intellectual analysis of data. At this stage, hazards become risks that can be implemented into the logic of managerial decision-making. Optimal IT risk management involves online monitoring of numerous parameters that affect the possibility of risks and determine their consequences. The risks that banks face using IT solutions extend to third-party IT providers that many banks rely on for cloud storage and other services. These systems can slow down or fail, preventing customers from accessing ATMs or mobile apps. Even the speed of a technological change creates operational risk. In connection with the above, the automation of operational risk management based on the use of intelligent technologies is one of the most urgent tasks for credit institutions. The authors suggest that the networks can be trained on statistical data specific to each institution to enable accurate forecasting and event analysis using complex neural network technologies. The study identified models that demonstrated accurate results (it is necessary to take into account some limitations stated by the authors) on the training set formed by experts, leading to an expected increase in forecast accuracy by at least 40% upon implementation. The practical recommendations offered in the study have the potential to improve risk management practices and enhance the efficiency of credit organizations.

Keywords: *IT Risks, Artificial Neural Network, Machine Learning, Feedforward Neural Network, Keras High-Level Library (Framework).*

1. INTRODUCTION

In the decade following the global financial crisis, banks and their regulators have become more aware of the need to manage risks. Since rational risk management is fundamental to the management of any organization, it is an integral part of effective corporate governance.

Although banks have developed sophisticated financial risk control systems, they are still struggling to cope with operational risks, primarily due to the complexity of their identification and formalization.

In the International Convergence of Capital Measurement and Capital Standards, the Basel Committee on Banking Supervision defines operational risks as the risk of loss resulting from inadequate or failed internal processes, people, and systems or external events [1]. Although this definition does not formulate a set of criteria for separating operational risks from other types of banking risks, it can be used as a basis for building a methodology for the analysis and management of operational risks.

The main operational risk factors are related to [2,3]:

- Accidental or intentional actions of people or organizations against the interests of the organization, including non-compliance with legal requirements and internal rules and procedures;
- Imperfect organizational structures (the distribution of duties of departments and employees) and procedures, as well as their documentation, inefficient internal control, etc.;
- Failures in the functioning of systems and equipment;
- External circumstances beyond the control of the organization.

The measurement of operational risk requires an assessment of the likelihood of operating losses, as well as their potential size. Now banks mainly use analytical and evaluation methods to measure the level of operational risk [4,5].

Based on the use of neural networks, the article aims at organizing a system for managing the operational risks of a credit institution arising in the process of using IT technologies. This approach will significantly improve the efficiency and quality of decisions made in the field of operational risk management [6].

To achieve this objective, it is necessary to solve the following tasks:

1. To analyze the data collected by the credit institution in the event of operational risk, both mandatory (recommended) and possible for recording in the organization;
2. To determine the key risk indicators as input parameters in the classification of artificial neural networks and propose a generalized system for indicating the onset of operational risk;
3. To form training datasets;
4. To train (study) various models (frameworks) of networks and perform their comparative analysis.

In our opinion, the future development of bank operations will be effective when used proposes an innovative approach to assessing operational IT risk in credit institutions using artificial neural networks. The category of operational risk is important not only as an accumulating point for existing risk management practices but also as an emphasis on risks/threats that have either been ignored by banks or not reflected in management systems. From this perspective, operational risk is part of a broader understanding of risk identification for any risk management system and its inclusion in the agenda of managerial thinking.

2. METHODS

2.1 Study Design

In the course of the study, the classifier of operational loss events was analyzed in terms of sources and types of events, their impact on the continuity of critical business processes, and types of losses to identify significant fields (attributes) of the common (mandatory) part of the data and the base of events for the implementation of operational risk.

The main sources of operational loss events are as follows: the inefficient organization of business processes; actions of personnel and other persons associated with the credit institution; system and equipment failures; external causes (including the actions of third parties). The credit institution should record connections between the realized operational loss event and other types of risks resulting from the event, as well as determine the most significant of them [7-9].

Seven types of operational loss events were considered: deliberate actions of personnel, deliberate actions of third parties, damage to tangible assets, violation of personnel policy, violation and failures of systems and equipment, violation of customer rights, and violation of organization and process management [10,11].

As types of losses, we considered only losses determined in monetary terms (direct or reflected in the financial statements, and indirect or determined by the calculation method).

To ensure the universal approach, i.e. regardless of the type of event and its connection with other risks, it is proposed to assess the impact of an event on the continuity of business processes using an indication system. Its general structure contains two artificial neural networks: to determine the influence of associated risks and to indicate the criticality of a particular operational loss event. To determine the criticality and urgency of measures to mitigate the consequences of an operational risk event, the method of assigning the criticality status “red (critical) – amber (medium) – green (weak)” (RAG) is often used [2].

For this study, we selected the type of events associated with violations and failures of systems and equipment that ensure the functioning of a credit organization. Three experts from the Plekhanov Russian University of Economics formed a database of 21,600 events in various states and assessed the type of indication (green, amber, and red zones). When determining the level of risk criticality, the experts took into account the event’s connection with other types of risks.

From the viewpoint of the application of various artificial neural networks, two types were identified as the most suitable for this study: a feedforward network with one hidden layer (FNN) and a deep network, i.e. a multilayer perceptron with two, three, and four hidden layers (DNN) [5,12-14]. In these connections between the nodes, no cycles are formed, information moves only in one direction from the input nodes through the hidden nodes to the output nodes.

All experiments to study the listed types of networks and determine the optimal artificial neural network (number of hidden layers, number of neurons in a layer, activation function) were carried out using the high-level Keras library in Python, which allows a quick start at the initial stages of research and obtaining the first results [15].

2.2 Research Stages

At the initial stage of the study, we analyzed a typical database of credit organization events, containing information about the losses caused by operational risks. Based on the analysis, a list of attributes was identified that characterizes the state of business processes in terms of the need for preventive actions by personnel [16].

Based on the list of parameters obtained, the main data flow entering an artificial neural network is described at the next stage of the study. Considering the influence of associated risks leads to a variable number of input parameters (the number of neurons in the input layer). On the one hand, it is necessary to obtain a static artificial neural network. On the other hand, to avoid a double analysis of one event from the viewpoint of different risks, it is proposed to conduct a preliminary analysis of associated risks using an additional feedforward neural network.

Thus, the system for indicating the state of business processes in the implementation of operational risks includes two artificial neural networks. To determine the level of criticality, an artificial neural network with nine input neurons is proposed. They process the criticality of the incident, the normalized deviation from the standard elimination time (from the moment of onset and detection), the types of (direct and indirect) losses that the event can lead to, the possibility of compensation losses, the exact time when the event occurred, the source of the event, the severity of the associated risks. Three output neurons are corresponding to the criticality of business processes (the classification indicators of the output layer are “red” (high), “amber” (medium), and “green” (low). To determine the criticality of associated risks, the 5-m-3 architecture was chosen. This receives the maximum direct and indirect losses, the maximum and minimum criticality among the associated risks, as well as the probability of direct and indirect losses [14,16].

Further, experimental cycles of training networks were carried out to determine the optimal artificial neural networks. The training process included samples of 1,000 and 21,600 sets for artificial neural networks to assess the criticality of associated risks and the criticality of business processes, respectively. The general sample was divided into a training sample, which accounted for 80% of the total number of training sets, and validation and test samples (10% each). Traditionally, learning has taken place epochwise.

To assess the criticality of associated risks within artificial neural networks, training was carried out for the number of neurons in the hidden layer m = 10, 15 (5-10-3 and 5-15-3 models). In addition, the size of the training sample allowed us to conduct experiments for two-layer models, in particular 5-10-10-3 [17,18].

According to general heuristic recommendations, to indicate the criticality of a business process, experiments were carried out for m = 14, 18, 24, 27 with one hidden layer and for m = 9, 14, 18, 24 with two-four hidden layers. The training was carried out for 200 epochs. SGD, Adam, and RMSprop implemented in Keras were compared as optimizers to achieve faster convergence. The sigmod, relu, and tanh (the hyperbolic tangent) functions were compared as the activation function of the hidden layer, while softmax is the activation function of the output layer. Together with the optimizer, the MSE loss function (the mean squared error) [18-20] was used.

3. RESULTS

3.1 The Model of an Artificial Neural Network

To organize preventive measures to combat and strengthen control at various stages of dealing with operational risks, regulatory state bodies recommend collecting and storing 50 mandatory parameters of an event that causes operational risks. Most of these parameters do not characterize the impact of the event on business continuity. As a result of their analysis, the attributes obtained after preliminary processing of some mandatory and additional (recommended for storage) parameters were determined, which allows us to assess the criticality of the current event.

In total, 10 attributes were allocated with their numerical interpretation as potential output parameters of an artificial neural network:

1. *Criticality* is the influence (green – low (1), amber – medium (2), red – high (3)) of an incident (event) on business processes that might lead to losses. The higher the ratio, the higher the risk, i.e. the event more often leads to losses or necessarily leads to significant losses;

2. *Overtime* to eliminate defects from *the moment of the event* normalized by a number from 0 (eliminated in the allowable time limit) to 1 (200% or more overtime). The allowable elimination time for a particular type of event is determined individually for each credit organization by the credit organization itself;

3. *Overtime* to eliminate defects from the moment the event was detected is defined in the same manner as in the previous paragraph;

4. *Direct losses* are the losses caused by a certain type of events during the period of statistics collection on a scale from 0 to 1, where 0 denotes insignificant losses (the threshold is set directly by the credit organization (P_{min}), 1 is the maximum loss recorded in the credit organization or occurred in the credit organization under a certain set of circumstances (P_{max});

It is possible to obtain a numerical value of the level of certain losses as a percentage of the average value of losses for a given type for the entire period of statistics collection using the following formula:

$$\frac{\frac{\sum P_i}{k} - P_{min}}{P_{min} - P_{max}} \quad (1)$$

where P is the amount of loss in monetary terms, k is the number of events of this particular type, P_{min} and P_{max} are the minimum and maximum losses for this type of event;

5. *Indirect losses* are a binary feature (0 or 1) showing whether this event can cause indirect losses (whether there were indirect losses during the collection of statistics);

6. *The time of day* when the event occurred (working or non-working);

7. *The day* when the event occurred (a working day or a day off);

8. *The source of the event* is a number from the directory (1-4: deficiencies in processes, actions of personnel and other persons, failures of systems and equipment, external causes);

9. *The type of the event* is a number from the directory (1-7: deliberate actions of personnel, deliberate actions of third parties, damage to tangible assets, violation of personnel policy, violation and failure of systems and equipment, violation of customer rights, violation of organization and process management);

10. *The feature of connection* with other types of risks (whether the event entails the onset of an indirect risk (several risks) and losses associated with it).

The influence of the event under consideration can extend to a different number of related risks. To implement a more universal approach (independent of the number of such links), we decided to use the criticality of emerging related risks as a sign of connectedness, which should be determined by a special artificial neural network [18,21]. As a result, a general view of information flows within the system for indicating the level of criticality of an event is shown in Figure 1.

To simplify the preparation of training data sets and a preliminary assessment of the system based on an artificial neural network, it was decided to study the proposed approach for only one type of event, namely, violations and failures of systems and equipment. Thus, the generalized model of an artificial neural network for determining the criticality of a realized event can be described by an input layer containing nine neurons and an output layer containing three neurons.

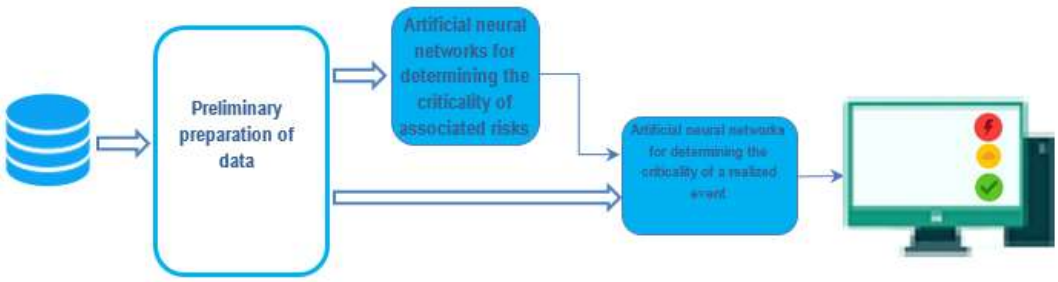

Figure 1: The General Structure of the System for Indicating the Criticality of a Realized Event

The determination of the criticality of associated risks is influenced by the following parameters, which are potential inputs to artificial neural networks:

1. The maximum direct losses among all associated risks, i.e. the value for a particular risk is determined by the formula similar to the direct losses evaluated for the main risk;

2. Indirect losses have the following values: 1 – can occur, 0 – do not occur among all associated risks;

3. The maximum criticality among the associated risks that can lead to losses (low, medium, high);

4. The minimum criticality among the associated risks;

5. The probability of direct losses is the average value of likelihood among all associated risks determined based on accumulated statistics as the ratio of the occurrence of a loss to the total number of events of a certain type.

Thus, the generalized artificial neural network for determining the criticality of associated risks can be described by an input layer containing five neurons and three neurons in the output as a criticality class (low, medium, high).

3.2 Training Artificial Neural Networks to Determine the Criticality of a Realized Event

To determine the optimal network structure, training experiments were carried out for feedforward networks with a different number of hidden layers and neurons in the hidden layer, as well as with different learning parameters: activation functions and weight update algorithms (optimizers). The results are summarized in Table 1. For all optimizers, the MSE loss function (the mean squared error) was used, whose value is indicated in brackets.

Table 1: Network Accuracy on the Test Sample

		Optimizer								
		Adam			SGD			RMSprop		
Activation function		relu	sigmoid	tanh	relu	sigmoid	tanh	relu	sigmoid	tanh
		Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)	Acc. (mse)
Models										
FNN										
One hidden layer	9-14-3	92.27 (0.05)	95.28 (0.03)	98.84 (0.007)	95.46 (0.036)	76.94 (0.12)	91.42 (0.047)	88.29 (0.07)	97.96 (0.01)	98.33 (0.009)
	9-18-3	96.85 (0.015)	99.31 (0.005)	97.87 (0.013)	95.09 (0.039)	77.08 (0.12)	92.29 (0.046)	90.51 (0.06)	98.47 (0.008)	98.5 (0.013)
	9-24-3	92.64 (0.047)	98.94 (0.006)	98.7 (0.007)	94.34 (0.037)	75.83 (0.12)	92.45 (0.048)	95.74 (0.023)	96.44 (0.023)	98.98 (0.005)
	9-27-3	98.33 (0.008)	99.44 (0.0035)	99.4 (0.003)	94.26 (0.036)	75.69 (0.12)	93.52 (0.046)	97.04 (0.018)	99.4 (0.003)	99.07 (0.005)
DNN										
Two hidden layers	9-9-9-3	93.06 (0.038)	97.31 (0.016)	98.19 (0.01)	95.19 (0.028)	71.02 (0.15)	95.28 (0.03)	97.31 (0.015)	98.24 (0.01)	97.22 (0.015)
	9-14-14-3	97.36 (0.014)	99.31 (0.003)	99.35 (0.004)	95.75 (0.026)	74.26 (0.014)	96.44 (0.027)	96.16 (0.02)	98.38 (0.008)	98.84 (0.007)
	9-18-18-3	98.43 (0.01)	99.72 (0.0013)	98.43 (0.01)	96.3 (0.027)	75.42 (0.13)	96.02 (0.028)	97.82 (0.012)	98.29 (0.01)	98.43 (0.01)
	9-24-24-3	95.42 (0.029)	99.95 ($2*10^{-4}$)	99.7 (0.0012)	96.39 (0.021)	75.00 (0.135)	96.16 (0.024)	98.29 (0.01)	98.75 (0.007)	99.58 (0.0027)
Three hidden layers	9-9-9-9-3	95.83 (0.025)	98.8 (0.0065)	97.64 (0.012)	95.6 (0.026)	55.14 (0.2)	95.88 (0.024)	90.97 (0.053)	98.29 (0.01)	96.85 (0.017)
	9-14-14-14-3	98.56 (0.009)	98.38 (0.008)	99.03 (0.005)	96.71 (0.021)	54.38 (0.209)	96.81 (0.027)	94.63 (0.03)	97.96 (0.011)	99.26 (0.004)
	9-18-18-18-3	98.33 (0.01)	99.77 (0.0013)	99.17 (0.0054)	97.0 (0.019)	53.8 (0.205)	97.11 (0.018)	96.3 (0.024)	98.52 (0.0077)	99.4 (0.004)
	9-24-24-24-3	95.93 (0.026)	99.12 (0.0045)	98.29 (0.01)	97.5 (0.018)	58.01 (0.19)	97.27 (0.017)	98.66 (0.007)	97.82 (0.012)	99.5 (0.002)
Four hidden layers	9-9-9-9-9-3	95.56 (0.023)	98.75 (0.0067)	98.84 (0.005)	92.92 (0.033)	42.22 (0.21)	97.22 (0.018)	90.28 (0.05)	96.99 (0.016)	97.87 (0.01)
	9-14-14-14-14-3	97.41 (0.014)	98.84 (0.0063)	97.59 (0.014)	96.88 (0.019)	42.22 (0.21)	97.02 (0.017)	97.73 (0.0126)	99.49 (0.004)	98.84 (0.006)
	9-18-18-18-18-3	96.81 (0.018)	99.81 (0.0012)	96.39 (0.018)	97.64 (0.013)	42.22 (0.21)	97.82 (0.015)	96.02 (0.024)	99.17 (0.004)	99.21 (0.004)

The presented results were obtained during training for 200 epochs. In this case, no retraining effect was observed. Figure 2 shows learning curves for the best version of the 9-24-24-3 network model.

Journal of Theoretical and Applied Information Technology
15th June 2023. Vol.101. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

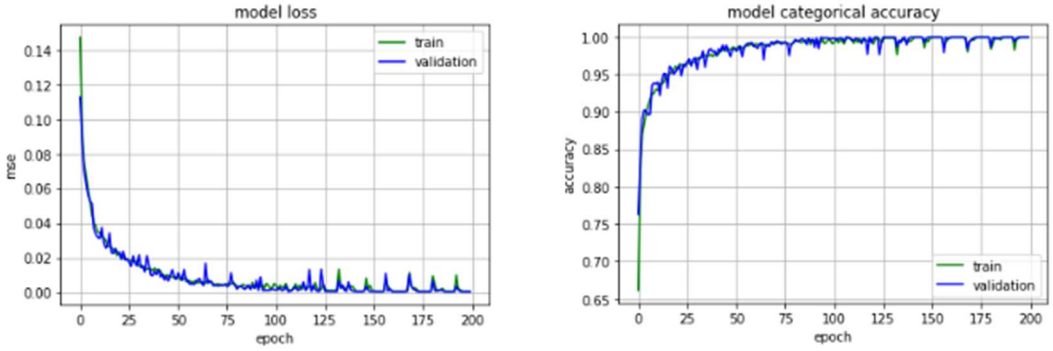

Figure 2: Learning Curves of Feedforward Neural Networks with 9-24-24-3 Architecture

The most surprising results were obtained when training a multilayer perceptron using the SGD optimizer in conjunction with the sigmoid activation function. For two layers, the accuracy of the network did not exceed 75%. With the addition of the third layer, it even decreased. The four-layer perceptron was practically not trained. An increase in the number of epochs did not improve the result.

3.3 Training Artificial Neural Networks to Determine the Criticality of Associated Risks

The artificial neural network for determining the criticality of associated risks acted as an auxiliary network which, among other things, was entrusted with the function of accounting for the criticality of all risks associated with a particular event [22,23]. In accordance with the heuristic recommendations and the volume of the general sample, we studied models with 5-10-3, 5-15-3, and 5-10-10-3 architectures. The training results are shown in Table 2. The training was carried out using the Adam optimizer and sigmoid activation functions since it demonstrated the best results for our task at the previous stage of the study.

Table 2: The Results of Training Artificial Neural Networks to Determine the Criticality of Associated Risks

Accuracy Model	Training accuracy	Accuracy on the control set	Accuracy on the test set
5-10-3	96.21	97.28	95.45
5-15-3	95.27	96.57	93.94
5-10-10-3	96.97	98.48	96.97
5-15-15-3	97.54	98.48	96.97

Two-layer architectures with 10 and 15 neurons per layer showed similar results in terms of accuracy. Figure 3 shows the learning curves of the 5-10-10-3 architecture with one of the best learning results.

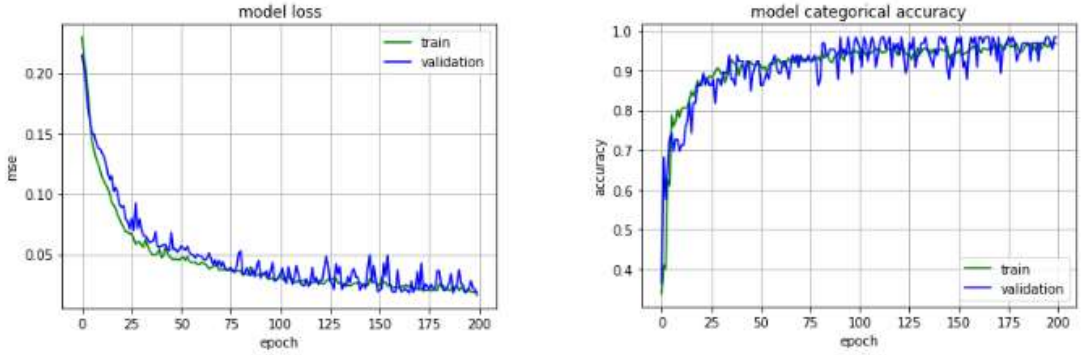

Figure 3: Learning Curves of Artificial Neural Networks Determining the Criticality of Associated Risks with 5-10-10-3 Architecture

The proposed models have shown fairly high accuracy (96%) and a further increase in network efficiency only by increasing the training set.

4. DISCUSSION

In general, the artificial neural networks under consideration have demonstrated high accuracy, in particular, 99% for determining the criticality of a realized event and 96% for determining the

criticality of associated risks. The proposed mechanism for private risk assessment based on artificial neural networks can be adapted considering the real functioning of credit organizations. The effectiveness of the proposed methodology can be further evaluated when it is tested based on a real risk management system [22,23]. By using a neural network to assess operational risk, credit institutions can reduce the costs associated with traditional risk assessment methods, such as hiring risk experts [5].

In the course of the study, parameters for assessing the criticality of an event (input parameters of neural networks) were proposed. At first glance, they are independent of the source of the event but they are purely informational. However, it is impossible to state this without additional analysis of the data characterizing certain types of events, in particular those associated with the actions of personnel and other external causes [6,9,24]. The researchers note, that operational loss data is often incomplete and not easily accessible. Therefore, the lack of sufficient data could limit the development of an accurate neural network [5].

As the results of the study show, most often researchers highlight the complexity of the model for its further development. Building a neural network requires a significant amount of computational resources, including powerful hardware and software tools. Therefore, the complexity of the model may be a limitation for organizations with limited computational resources [25]. Based on the availability of our resources, several assumptions were made for our study. One of them is related to the limited expert resources. The risk gradation had only three levels (red, yellow, and green). However, this division is inaccurate and can be insufficient in a real credit organization indicating the urgency of the response and the application of emergency measures. The second assumption is that only direct signal propagation networks were studied. Although they showed excellent results, it would be interesting to investigate how, for example, radial basis networks [24,26] perform in relation to the tasks being solved.

Throughout the study, little attention was paid to the relevant and complex task of assessing associated events and risks. It is necessary to evaluate the effectiveness of the proposed approach and assess whether it will exclude interrelated risks arising from various events, possibly even with modification of the network model.

5. CONCLUSION

The paper proposes a method for assessing the impact of operational IT risk using an artificial neural network. If necessary, it is assumed possible to train networks on statistical (preliminarily processed) data of a particular credit institution as a tool for setting up a network and analyzing events through the use of complex neural network technologies.

Models were selected that showed good results on the training set formed by experts. As a result, efficiency is expected to increase due to an increase in forecast accuracy by at least 40% after the introduction of a neural network.

The study results promote their widespread use by credit organizations. The above-mentioned recommendations in the field of identifying and resolving operational risks were formed based on practical observations and aim at real results upon implementation.

While building a neural network to assess the level of operational risks of a credit institution has some limitations, such as data availability and quality, model complexity, and interpretability, it also has many prospects, including improved accuracy, real-time monitoring, reduced costs, and improved decision-making.

REFERENCES:

[1] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework. Electronic text data*, November 2005. [Online]. Available: https://www.bis.org/publ/bcbs118.pdf

[2] S. Ashby, *Fundamentals of operational risk management: understanding and implementing effective tools, policies and framed*. 1st ed. Kogan Page, 2022.

[3] A.M.A.M. Al-Sartawi (Ed.), *Artificial intelligence for sustainable finance and sustainable technology*. Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-93464-4

[4] A.A. Kazimagomedov, *Bankovskoe delo: organizatsiya deyatelnosti tsentralnogo banka i kommercheskogo banka, nebankovskikh organizatsii* [Banking: the activities of the central bank and commercial bank, non-banking organizations]: student's textbook. INFRA-M, Moscow, 2017, 502 p.

[5] M. Tavana, A.-R. Abtahi, D. Di Caprio, and M. Poortarigh, "An artificial neural network and

bayesian network model for liquidity risk assessment in banking", *Neurocomputing*, Vol. 275, 2018, pp. 2525-2554. https://doi.org/10.1016/j.neucom.2017.11.034

[6] O.S. Zinisha, and N.R. Petrov, "Primenenie iskusstvennogo intellekta v bankovskoi sfere [The use of artificial intelligence in the banking sector]", *Colloquium-Journal*, No. 1(7), 2019, pp. 38-42.

[7] L.R. Magomaeva, "Ekonomicheskaya paradigma i zadachi kreditno-finansovogo sektora v usloviyakh bolshikh dannykh i tekhnologii oblachnykh servisov [Economic paradigm and tasks of the credit and financial sector in the context of big data and cloud service technologies]", *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta imeni Kosta Levanovicha Khetagurova*, No. 1, 2019, pp. 102-106. https://doi.org/10.29025/1994-7720-2019-1-102-106

[8] S. Wang, and Z. Zhao, "Risk decision analysis of commercial insurance based on neural network algorithm", *Neural Computing & Applications*, Vol. 35, 2022, pp. 2169-2182.

[9] N.E. Sokolinskaya (Ed.), *Sovremennye problemy i perspektivy upravleniya riskami bankov* [Modern problems and prospects of bank risk management]: the collection of scientific works by Master's Degree students. Rusains, Moscow, 2017, 102 p.

[10] I.J. Jacob, S.K. Shanmugam, and I. Izonin (Eds.), *Data intelligence and cognitive informatics*. Springer, Singapore, 2023. https://doi.org/10.1007/978-981-19-6004-8

[11] W. Kratsch, J. Manderscheid, M. Roglinger, and J. Seyfried, "Machine learning in business process monitoring: a comparison of deep learning and classical approaches used for outcome prediction", *Business & Information Systems Engineering*, Vol. 63, 2021, pp. 261-276. https://doi.org/10.1007/s12599-020-00645-0

[12] O.A. Gureeva, and M.S. Potapova, "Obuchayushchie i testovye dannye dlya neironnykh setei [Training and testing data for neural networks]", *Nauka i studia*, Vol. 1, No. 3, 2017, pp. 75-77.

[13] Rahulbansal, *Radial Basis Function Network*, February 6, 2017. [Online]. Available: https://www.hackerearth.com/blog/developers/radial-basis-function-network/ (assessed date: January 15, 2023).

[14] E.A. Trofimova, V.D. Mazurov, and D.V. Gilev, *Neironnye seti v prikladnoi ekonomike* [Neural networks in applied economics]. Izd-vo UrFU, Yekaterinburg, 2017, 96 p.

[15] M.V. Zaginailo, "Primenenie metodov matematicheskoi statistiki dlya otsenki zaklyuchenii iskusstvennoi neironnoi seti v zadache raspoznavaniya obrazov [Application of mathematical statistics methods to evaluate the conclusions of an artificial neural network on pattern recognition]", *Alleya Nauki*, Vol. 3, No. 1, 2019, pp. 1006-1012.

[16] M. Peihani, "Regulation of cyber risk in the banking system: a Canadian case study", *Journal of Financial Regulation*, Vol. 8, No. 2, 2022, pp. 139-161.

[17] D.S. Kurnikov, and S.A. Petrov, "Ispolzovanie neironnykh setei v ekonomike [The use of neural networks in economics]", *Juvenis Scientia*, Vol. 6, 2017, pp. 10-12.

[18] Y.V. Bodyanskiy, A.K. Tyshchenko, and A.A. Deineko, "An evolving radial basis neural network with adaptive learning of its parameters and architecture", *Automatic Control and Computer Sciences*, Vol. 49, 2015. pp. 255-260.

[19] R. Chandradevan, *Radial Basis Functions Neural Networks — All we need to know*, August 18, 2017. [Online]. Available: https://towardsdatascience.com/radial-basis-functions-neural-networks-all-we-need-to-know-9a88cc053448 (assessed date: January 15, 2023).

[20] D.K. Nguyen, H.J. von Mettenheim, and C. Stasinakis, "Preface: neural networks, nonlinear dynamics, and risk management in banking and finance", *Annals of Operations Research*, Vol. 297, 2021, pp. 1-2. https://doi.org/10.1007/s10479-020-03893-1

[21] A.Sh. Galiullina, A.P. Vasilev, I.A. Kovalenko, and A.A. Sbitneva, "Iskusstvennye neironnye seti [Artificial neural networks]", *Teoriya. Praktika. Innovatsii*, No. 1(37), 2019, pp. 29-33.

[22] A. Zell, *Simulation neuronaler netze* [The modeling of neural networks]. 1st ed. Addison-Wesley, Bonn, 1994, p. 73.

[23] A. Patra, S. Das, S.N. Mishra, and M.R. Senapati, "An adaptive local linear optimized radial basis functional neural network model for financial time series prediction", *Neural Computing & Applications*, Vol. 28, 2017, pp. 101-110.

[24] J. Schmidhuber, "Deep learning in neural networks: An overview", *Neural Networks*, Vol.

61, 2015, pp. 84-117. https://doi.org/10.1016/j.neunet.2014.09.003

[25] N.C. Thompson, K.H. Greenewald, K. Lee, and G.F. Manso, "The Computational Limits of Deep Learning", *ArXiv*, Vol. 2007, 2020, 05558. https://doi.org/10.48550/arXiv.2007.05558

[26] P. Shukla, and R. Iriondo, *A tutorial on the main types of neural networks and their applications to real-world challenges*, July 13, 2020. [Online]. Available: https://towardsai.net/p/machine-learning/main-types-of-neural-networks-and-its-applications-tutorial-734480d7ec8e