https://doi.org/10.29042/2020-10-5-133-140

Helix (2020) 10 (5): 133-140

Definition of Phishing Sites Based on the Team Model of Fuzzy Neural Networks

✉ [1] **Ilyas Idrisovich Ismagilov, [2]Aynur Ayratovich Murtazin, [3] Dina Vladimirovna Kataseva, [4]Alexey Sergeevich Katasev, [5]Andrey Igorevich Barinov**

[1]Department of Economic Theory and Econometrics, Institute of Management, Economics and Finance, Kazan Federal University
iiismag@mail.ru
[2] Institute of Management, Economics and Finance, Kazan Federal University
Ainur-murt@bk.ru
[3,4,5] Department of Information Security Systems, Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A.N. Tupolev "KAI"
DVKataseva@kai.ru
ASKatasev@kai.ru
antenor2002@gmail.com

Received: 21st August 2020, Accepted: 14th September 2020, Published: 31st October 2020

Abstract

This paper solves the problem of defining phishing sites based on building a team model of fuzzy neural networks (FNNs). The main methods of phishing are analyzed. Attention is drawn to the fact that phishing has become widespread on the Internet through the use of phishing sites. The expediency of identifying phishing sites based on the analysis of their URLs is noted. The main approaches to identifying phishing sites are described. The need to implement an approach based on machine learning by constructing fuzzy neural networks for the creation of fuzzy knowledge bases and their use to identify phishing sites is actualized. Automating the identification of phishing sites based on the neuro-fuzzy approach required solving the problems of collecting and preparing initial data for analysis, building a team model of fuzzy neural networks, and forming a fuzzy knowledge base, as well as conducting research, and assessing the accuracy of identifying phishing sites based on the constructed model. The initial data was formed from various sources. The total amount of initial data was 50,000. Of these, 10 input features for analysis were selected by an expert. After carrying out the correlation analysis, 4 most informative input features were selected for analysis: site lifetime, site rank, URL length, and the registered status of the site. An output feature of the site was its type: phishing or legitimate. After assessing the quality and cleaning the selected data, the resulting sample was formed of 34718 rows, of which 70% were used for learning (24303 rows), and 30% (10415 rows) for testing. A team model of fuzzy neural networks was built and a knowledge base was formed on the basis of the data obtained, including 4608 fuzzy rules. Studies have shown that the number of errors of the 1st type in identifying phishing sites is 2.01%, and 2.89% for errors of the 2nd type. The general classification error based on knowledge base rules is 4.9%. The accuracy of identifying phishing sites was 95.1%, which exceeds the accuracy of other classification methods: multilayer neural network, decision tree, linear and logistic regression. The knowledge base formed on the basis of the team model of fuzzy neural networks can be effectively used to identify phishing sites on the Internet.

Keywords

Phishing Site, Knowledge Base, Fuzzy Neural Network, Team Model of Fuzzy Neural Networks, Classifier, Data Mining

Introduction

As is known, phishing is a type of fraud where an attacker contacts a victim under the guise of a real organization in order to obtain confidential information (Lakhita & Bohra, 2015). There are the following main phishing methods (Chuchuen & Chanvarasuth, 2015):

- Voice Phishing - an attacker tries to gain access to confidential information of bank customers through telephone communication under various pretexts in order to steal their funds;
- SMS Phishing - distribution of SMS messages containing links that lead to phishing sites (scammers receive confidential information due to the fact that victims follow the links specified in the SMS messages and enter their personal data there);
- Spear Phishing - sending emails to specific users (unlike traditional phishing, in which many emails are sent to unknown users, the spear phishing technique is targeted);

- Phishing in search engines - a technique, in which there is created a fake web page indexed in a search engine for certain keywords.

Phishing has become widespread on the Internet through the use of phishing sites (Purkait et al., 2014). Such sites are created to allow an attacker to gain access to confidential user data. Most phishing methods use disguised fake links to phishing sites that lead to a copy of an original site of a company. Cybercriminals most often use Internet addresses in which they deliberately enter typos. The creation of phishing sites not only brings financial losses, but also significantly reduces the credibility of the company among its clients. Therefore, the creation of new effective methods of combating phishing sites will help protect the authority of companies, their financial resources, as well as reduce the risk of confidential user data getting to cybercriminals.

One of the most common phishing techniques is to use obfuscated URLs to redirect users to phishing sites that look similar to the original company sites. At the same time, it is not difficult for cybercriminals to lure users into clicking on fraudulent links.

To deal with this threat, the best strategy is to discourage people from connecting to phishing sites by identifying phishing URLs. Most of the countermeasures in this area are based on the use of databases with phishing sites. However, they proved to be ineffective due to the short lifetime of the site (Fu-An, 2015; Patil et al., 2020). Hence, real-time detection of malicious URLs is relevant. In this paper, to solve this problem, an approach is proposed based on the construction of a team model of fuzzy neural networks (Chupin et al., 2019), the formation and use of a fuzzy knowledge base (Katasev, 2019).

Methods

Currently, there are three main approaches to the classification of phishing sites (Kosuri & Nagasri, 2020). The first approach is manual classification. The essence of the approach is that experienced and trained users independently determine whether a site is phishing. The criterion for determining can be the use of a similar URL (for example, "onllinesberbank.ru" or "online.sbrbank.ru" is used instead of "online.sberbank.ru"), the absence of an SSL certificate, grammatical or spelling errors, etc. This classification is not always effective, since not all users have sufficient knowledge, experience, and qualifications to identify phishing sites.

The second approach is to use keywords that are on the page of the site and validate them in a search engine (e.g. Google). If the site checked is in the top lines of the search engine results, then the site will be considered legitimate, otherwise it is phishing. Unlike the first approach, this approach can be automated. However, this requires sufficient processing power and a large amount of time, since it is necessary to crawl each web page and analyze the content of the search query for keywords classify a large number of sites.

The third approach uses machine learning algorithms (Singh & Ashraf, 2019; Satapathy et al., 2019). There are two types of learning: precedent learning (based on identifying patterns in the analyzed data) and deductive learning (this involves formalizing expert knowledge and forming knowledge base on its basis).

The use of machine learning methods is the most relevant among these approaches (Perfilieva et al., 2016; Dagaeva et al., 2019; Katasev et al., 2018). At the same time, a promising area of research in this approach is the development of methods that combine the advantages of learning proceeding from precedents with the advantages of deductive learning. One of the implementations of this concept is the use of fuzzy neural networks (ALmomani et al., 2012). The relevance of their application lies in the fact that a trained fuzzy neural network allows us to form a fuzzy knowledge base, on the basis of which an effective solution to the problem of identifying phishing sites with the interpretation of the result in natural language is possible.

Automating the identification of phishing sites within the neuro-fuzzy approach required solving the following tasks:

- Collection and preparation of initial data for analysis;
- Construction of a FNN team model and forming a fuzzy knowledge base;
- Conducting research and assessing the accuracy of identifying phishing sites based on the model constructed.

In the paper, we used two datasets corresponding to phishing and legitimate sites to build a FNN team model. The data was compiled from various sources. PhishTank data (Bell & Komisarczuk, 2020) was used as a source of phishing sites. Users publish links there that are suspected of phishing, and other users vote on whether this resource is phishing or not. PhishTank is used in many modern browsers as well as add-ons for the Google Chrome browser. All PhishTank data is free to download or access via API calls. The collected data on phishing sites made up a set of 25,000 unique URLs.

To obtain a set of data on legitimate sites, two sources were used: Alexa Internet and Common Crawl. Alexa is a subsidiary of Amazon.com and is known for its site alexa.com, which collects statistics on traffic to third-party sites. This service collects information from users who have installed AlexaToolbar for their sites. The list of legitimate sites was uploaded using the Alexa Top Sites service. Common Crawl is a non-profit organization; it crawls monthly the Internet and makes its archives and datasets available to the public for free. The Common Crawl Web Archive consists of petabytes of data collected since 2011 (Chiniah et al., 2019). To obtain the URLs of legitimate sites, we used our own utility written in the Phyton language (Hao & Ho, 2019). As a result, data on 25,000 legitimate sites was collected. Thus, the total amount of raw data in the form of URLs of phishing and legitimate sites was 50,000.

10 input features for analysis were selected from the original dataset by an expert method:
1) Site rank (determined using the Alexa Top Sites service);
2) Is the URL an IP address (if the link has the structure of an IP address, then this parameter is assigned the value 1);
3) Whether the domain is registered (the site has been registered);
4) Lifetime (how many days the site has existed since registration);
5) The URL length (the number of all characters in the URL);
6) The presence of the "@" symbol in the link;
7) Whether the link is a redirect;
8) The presence of a dash in the domain name;
9) Domain length (number of characters in a domain name);
10) The number of subdomains in the URL.

The exit sign (phishing (1) or legitimate (0)) is the type of site.

A correlation analysis of the dependence of inputs on an output was carried out on the basis of calculating the Pearson correlation coefficient to assess the information content of the input features and reduce the dimension of the input feature space (Jebarathinam et al., 2020). The significance threshold was set at 0.25. The values of the correlation coefficient are presented in table 1.

Table 1: Values of the Coefficient Correlating Input Features with Output Features

Input feature No.	Name of input feature	Correlation coefficient
4	Site lifetime (activeDuration)	-0,523
1	Site rank (ranking)	0,517
5	URL Length (URLLen)	0,397
3	Availability of registration at the site (valid)	-0,267
8	The presence of dashes in the domain name (haveDash)	0,24
9	Domain Length (domainLen)	0,232
10	The number of subdomains in the URL (numOfSubdomain)	0,113
7	Is the link redirected (isredirect)	0,073
6	The presence of the symbol "@" in the link (is@)	0,04
2	Is the URL ip address (isIp)	0,013

Correlation analysis made it possible to select the following informative input features for analysis: site lifetime (activeDuration), site rank (ranking), URL length (urlLen), and site registration (valid). Data for the rest of the criteria were excluded. The procedures for assessing their quality and clearing (excluding lines with outliers and anomalous values) were applied to the remaining data. The resulting data sample was 34718 lines for 4 input and 1 output features. From the data obtained, 70% of the data (24303 lines) was randomly selected for the FNN learning, the remaining 30% (10415 lines) was selected for testing.

Based on the data obtained, a team model of fuzzy neural networks was constructed according to the bagging scheme (Smaida & Yaroshchak, 2020) using the bootstrap method (Akhmetvaleev & Katasev, 2018; Efron & Tibshirani, 1997) (see Fig. 1).

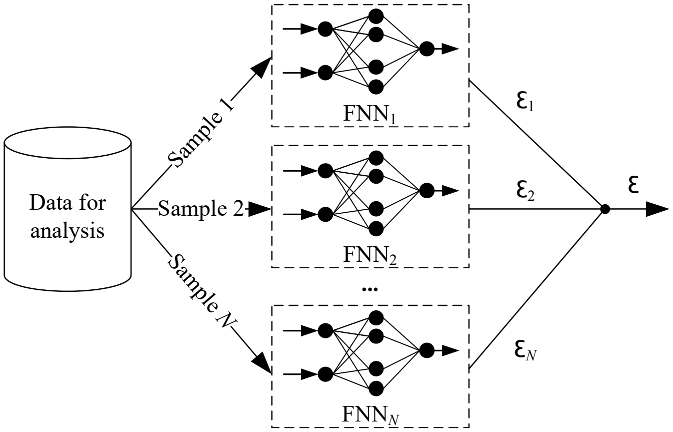


Figure 1: The Structure of the Team Model of Fuzzy Neural Networks

As can be seen from the figure, each FNN is learnt on the basis of the corresponding randomly generated data sample. Moreover, each FNN has its own bootstrap error ε_i, i = 1…N. The final bootstrap error ε of the team model is calculated as the averaged value of bootstrap errors of all FNN (Katasev, 2019).

The FNN team model generates a knowledge base in the form of a set of fuzzy rule system (Katasev, 2019). Figure 2 shows a knowledge base formation diagram.

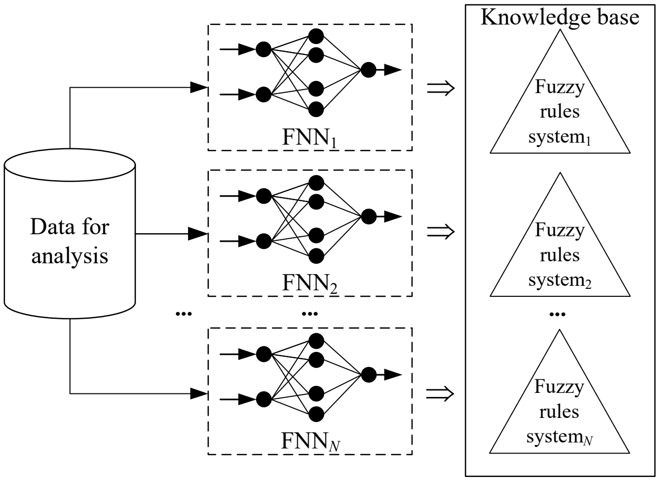


Figure 2: Knowledge Base Formation Diagram

In this diagram, each fuzzy neural network forms a system of fuzzy rules corresponding to it as a result of training; the rules together constitute a knowledge base. Moreover, each formed system of rules has its own classifying ability, since the process of training and testing the corresponding fuzzy neural networks is performed using different (random) data samples.

A fuzzy inference diagram based on the rules of the knowledge base has been implemented for a practical solution to the problem of identifying phishing sites. This fuzzy inference diagram is shown in Figure 3.

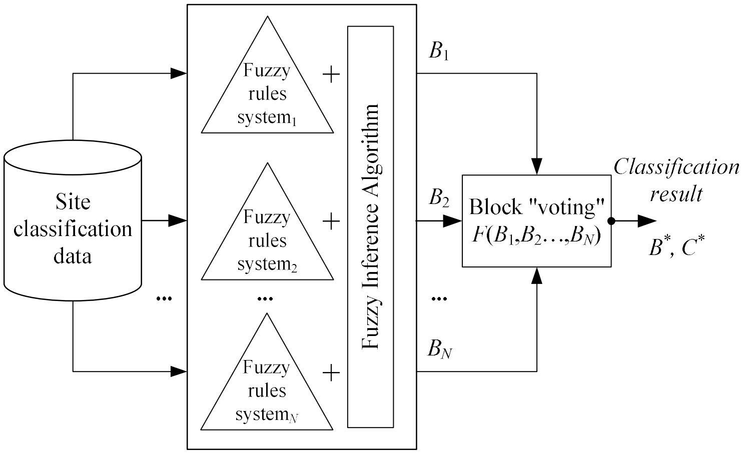
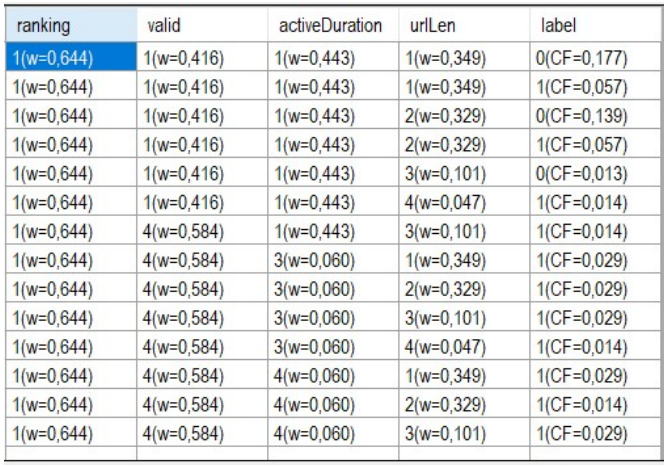


Figure 3: Site Classification Diagram based on the Knowledge Base

The following designations are used in the figure: F (B_1, B_2,…, B_N) - voting rules (Mustafin et al., 2018), B *∈ {1, 0} - site type, C * - assessment of the reliability of determining the site type.

Results and Discussion

A knowledge base was formed as a result of building a team model of fuzzy neural networks; a fragment of the base is shown in Figure 4.



ranking	valid	activeDuration	urlLen	label
1(w=0,644)	1(w=0,416)	1(w=0,443)	1(w=0,349)	0(CF=0,177)
1(w=0,644)	1(w=0,416)	1(w=0,443)	1(w=0,349)	1(CF=0,057)
1(w=0,644)	1(w=0,416)	1(w=0,443)	2(w=0,329)	0(CF=0,139)
1(w=0,644)	1(w=0,416)	1(w=0,443)	2(w=0,329)	1(CF=0,057)
1(w=0,644)	1(w=0,416)	1(w=0,443)	3(w=0,101)	0(CF=0,013)
1(w=0,644)	1(w=0,416)	1(w=0,443)	4(w=0,047)	1(CF=0,014)
1(w=0,644)	4(w=0,584)	1(w=0,443)	3(w=0,101)	1(CF=0,014)
1(w=0,644)	4(w=0,584)	3(w=0,060)	1(w=0,349)	1(CF=0,029)
1(w=0,644)	4(w=0,584)	3(w=0,060)	2(w=0,329)	1(CF=0,029)
1(w=0,644)	4(w=0,584)	3(w=0,060)	3(w=0,101)	1(CF=0,029)
1(w=0,644)	4(w=0,584)	3(w=0,060)	4(w=0,047)	1(CF=0,014)
1(w=0,644)	4(w=0,584)	4(w=0,060)	1(w=0,349)	1(CF=0,029)
1(w=0,644)	4(w=0,584)	4(w=0,060)	2(w=0,329)	1(CF=0,014)
1(w=0,644)	4(w=0,584)	4(w=0,060)	3(w=0,101)	1(CF=0,029)

Figure 4: Fragment of the Generated Knowledge Base

The total volume of the knowledge base was 4608 fuzzy rules. Let us consider the results of using a team model of fuzzy neural networks and a generated knowledge base to solve the problem of identifying phishing sites.

The accuracy of identifying phishing sites was assessed using a test sample of 10,415 lines. Approximately 50% of this data identified phishing sites (5,217 lines), the remaining 50% were for legitimate sites (5198 lines). The results of assessing the accuracy of site classification based on the generated knowledge base are presented in Table 2.

Table 2: Results for Site Classification based on a Test Data Sample

Actual values	Classified by the model		
	0	1	Total
0	5048	150	5198
1	105	5112	5217
Total	5153	5262	10415

In the table, the number "1" stands for "phishing site" and the number "0" for "legitimate site".

Based on the results obtained, the calculation of errors of the 1st and 2nd kind, as well as for the general classification error (see Table 3) was made.

Table 3: Classification Errors

1st kind errors, %	2nd kind errors, %	Total error, %
2,01	2,89	4,9

As can be seen from the table, the number of errors of the first kind was 2.01%, and the number of the errors of the second kind was 2.89%. In addition, the general classification error on the knowledge base rules was 4.9%, which is a high result in fuzzy modeling systems.

To increase the significance of the results obtained, the classification accuracy was compared on the basis of the generated knowledge base with the accuracy of other classification methods: multilayer neural network (Mukhametzyanov et al., 2019; Anikin et al., 2016; Emaletdinova & Kabirova, 2019; Ismagilov et al., 2018; Ismagilov et al., 2019), decision tree (Alqam & Zaro, 2019), linear and logistic regression (Asar & Wu, 2020). These classifiers were built and tested using the corresponding data samples in the Deductor modeling environment (Lomakin et al., 2019). Table 4 shows the results of the achieved classification accuracy.

Table 4: Comparison of Classification Accuracy based on Various Methods

Classification method	Classification accuracy, %
Multilayer neural network	92,75
Decision tree	92
Linear regression	90
Logistic Regression	87
Fuzzy knowledge base	95,1

As can be seen from the presented table, when building a FNN team model and forming a knowledge base, the highest accuracy in identifying phishing sites on the Internet is achieved.

The knowledge base formed on the basis of building a team model of fuzzy neural networks can be used as an additional extension in browsers for accurate identification of phishing sites on the Internet. In addition to determining the type of site, this model allows us to determine the criteria on the basis of which this decision was made.

Figure 5 shows a possible diagram for identification of phishing sites based on the generated knowledge base and a team model of fuzzy neural networks.

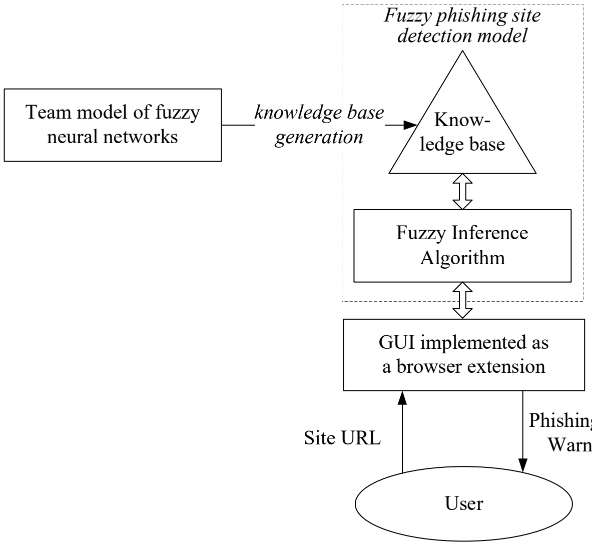

Fuzzy phishing site detection model
Team model of fuzzy neural networks
knowledge base generation
Know-ledge base
Fuzzy Inference Algorithm
GUI implemented as a browser extension
Site URL
Phishing Site Warning
User

Figure 5: Diagram of the Module for Identifying Phishing Sites

As we can see from the figure, the FNN team model built allows us to form a knowledge base, which, using the fuzzy inference module, is used to identify phishing sites. The initial data for determining the type of site is the URL entered by the user into the browser line. When the user visits a phishing site, the system should warn him and block access to the site's content. Unlocking access is possible when the user confirms that he still wants to visit the site. Also, the user can inform the developer that the state of the object (site) was determined incorrectly. This information will help improve the model for identifying phishing sites.

Summary

As the study has shown, , it is advisable to use modern machine learning methods in order to identify phishing sites on the Internet, namely, fuzzy neural networks that allow us to form fuzzy knowledge bases for classification. The results of assessing the accuracy of site classification based on various data mining methods allow us to conclude that the most effective tool for identifying phishing sites is a generated knowledge base. It allows us to minimize the number of errors of the first and second kind. In addition, the total error of this model does not exceed 5%, which is an acceptable result. The accuracy of classification based on a multilayer neural network, decision tree, and linear and logistic regression is inferior to the accuracy of classification of phishing sites based on a fuzzy knowledge base.

Conclusions

Thus, the work has solved the problem of identifying phishing sites on the Internet based on the building of a team model of fuzzy neural networks, as well as based on the formation and study of the effectiveness of a fuzzy knowledge base. The results of the studies have shown the effectiveness of the proposed approach to solving the problem. The generated knowledge base showed high accuracy in terms of minimizing errors of the first and second kind, as well as the general error of the model. This indicates its effectiveness and the possibility of practical use for identifying phishing sites on the Internet.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

References

[1] Akhmetvaleev, A.M., & Katasev, A.S. (2018). Neural network model of human intoxication functional state determining in some problems of transport safety solution. *Computer Research and Modeling,* 10(3), 285-293.

[2] ALmomani, A., Wan, T.-C., Altaher, A., ALomari, E., & Ramadass, S. (2012). Evolving fuzzy neural network for phishing emails detection. *Journal of Computer Science*, 8(7), 1099-1107.

[3] Alqam, S.J., & Zaro, F.R. (2019). Power quality detection and classification using s-transform and rule-based decision tree. *International Journal of Electrical and Electronic Engineering and Telecommunications,* 8(1), 45-50.

[4] Anikin, I.V., Makhmutova, A.Z., & Gadelshin, O.E. (2016). *Symmetric encryption with key distribution based on neural networks.* – 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM– Proceedings, 7911640.

[5] Asar, Y., & Wu, J. (2020). An improved and efficient biased estimation technique in logistic regression model. *Communications in Statistics - Theory and Methods,* 49(9), 2237-2252.

[6] Bell, S., & Komisarczuk, P. (2020). An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank. *ACM International Conference Proceeding Series.* a3.

[7] Chiniah, A., Chummun, A., Burkutally, Z., & Categorising, A.W.S. (2019). *Common Crawl Dataset using MapReduce*. 2nd International Conference on Next Generation Computing Applications 2019, NextComp– Proceedings, 8883665.

[8] Chuchuen, C., & Chanvarasuth, P. (2015). Relationship between phishing techniques and user personality model of Bangkok internet users. *Kasetsart Journal - Social Sciences,* 36(2), 322-334.

[9] Chupin, M.M., Katasev, A.S., Akhmetvaleev, A.M., & Kataseva, D.V. (2019). Neuro-fuzzy model in supply chain management for objects state assessing. *International Journal of Supply Chain Management,* 8(5), 201-208.

[10] Dagaeva, M., Garaeva, A., Anikin, I., Makhmutova, A., & Minnikhanov, R. (2019). Big spatiotemporal data mining for emergency management information systems. *IET Intelligent Transport Systems,* 13(11), 1649-1657.

[11] Efron, B., & Tibshirani, R. (1997). Improvements on cross-validation: The .632+ bootstrap method. *Journal of the American Statistical Association,* 92(438), 548-560.

[12] Emaletdinova, L.Y., & Kabirova, A.N. (2019). Methods of Constructing the Neural Network Models of Regulators for Controlling a Dynamic Object with Smooth Monotonous Behavior. *Russian Aeronautics,* 62(2), 213-221.

[13] Fu-An, Z. (2015). Phishing sites and prevention measures. *International Journal of Security and its Applications,* 9(1), 1-10.

[14] Hao, J., & Ho, T.K. (2019). Machine Learning Made Easy: A Review of Scikit-learn Package in Python Programming Language. *Journal of Educational and Behavioral Statistics,* 44(3), 348-361.

[15] Ismagilov, I.I., Khasanova, S.F., Katasev, A.S., & Kataseva, D.V. (2018). Neural network method of dynamic biometrics for detecting the substitution of computer. *Journal of Advanced Research in Dynamical and Control Systems,* 10(10 Special Issue), 1723-1728.

[16] Ismagilov, I.I., Molotov, L.A., Katasev, A.S., & Kataseva, D.V. (2019). Construction and efficiency analysis of neural network models for assessing the financial condition of enterprises. *Journal of Advanced Research in Dynamical and Control Systems*, 11(8 Special Issue), 1842-1847.

[17] Jebarathinam, C., Home, D., & Sinha, U. (2020). Pearson correlation coefficient as a measure for certifying and quantifying high-dimensional entanglement. *Physical Review A,* 101(2), 022112.

[18] Katasev, A.S. (2019). Neuro-fuzzy model of fuzzy rules formation for objects state evaluation in conditions of uncertainty. *Computer Research and Modeling,* 11(3), 477-492.

[19] Katasev, A.S., Emaletdinova, L.Y., & Kataseva, D.V. (2018). Neural network model for information security incident forecasting. *Proceedings - International Conference on Industrial Engineering, Applications and Manufacturing,* ICIEAM 2018, 8728734.
[20] Kosuri, N.K., & Nagasri, B. (2020). Phishing web sites features classification based on extreme learning machine. *Test Engineering and Management,* 83, 1222-1225.
[21] Lakhita, Y.S., & Bohra, B. (2015). Pooja A review on recent phishing attacks in Internet. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things*, ICGCIoT, 7380669, 1312-1315.
[22] Lomakin, N., Shokhnekh, A., Sazonov, S., Lukyanov, G., & Gorbunova, A. (2019). Hadoop and Deductor based digital ai system for predicting cost of innovative products in conditions of digitalization of economy. *ACM International Conference Proceeding Series,* 3373810.
[23] Mukhametzyanov, F., Katasev, A.S., Akhmetvaleev, A.M., & Kataseva, D.V. (2019). The neural network model of DDoS attacks identification for information management fail. *International Journal of Supply Chain Management,* 8(5), 214-218.
[24] Mustafin, A.N., Katasev, A.S., Akhmetvaleev, A.M., & Petrosyants, D.G. (2018). Using Models of Collective Neural Networks for Classification of the Input Data Applying Simple Voting. *Journal of Social Sciences Research,* 5, 333-339.
[25] Patil, N.M., Dias, S.P., Dcunha, A.A., Dodti, R.J. (2020). Hybrid phishing site detection. *International Journal of Advanced Science and Technology,* 29(6 Special Issue), 2452-2459.
[26] Perfilieva, I.G., Yarushkina, N.G., Afanasieva, T.V., & Romanov, A.A. (2016). Web-based system for enterprise performance analysis on the basis of time series data mining. *Advances in Intelligent Systems and Computing,* 450, 75-86.
[27] Purkait, S., De Kumar, S., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. Information Management and Computer Security, 22(3), 194-234.
[28] Satapathy, S.K., Mishra, S., Mallick, P.K., Gudur, R.R., & Guttha, S.C. (2019). Classification of Features for detecting Phishing Web Sites based on Machine Learning Techniques. *International Journal of Innovative Technology and Exploring Engineering*, 8(8), 425-430.
[29] Singh, D.K., & Ashraf, M. (2019). Detect the phishing websites in the context of internet security by using machine learning approach. *International Journal of Advanced Science and Technology,* 27(1), 104-111.
[30] Smaida, M., & Yaroshchak, S. (2020). Bagging of convolutional neural networks for diagnostic of eye diseases. *CEUR Workshop Proceedings,* 2604, 715-729.