2021
Vol.24 No.2

POLISH JOURNAL OF MANAGEMENT STUDIES
Kuzmenko O.V., Kubálek, J., Bozhenko V.V., Kushneryov O.S., Imre Vida.

AN APPROACH TO MANAGING INNOVATION TO PROTECT FINANCIAL SECTOR AGAINST CYBERCRIME

Kuzmenko O.V., Kubálek, J., Bozhenko V.V., Kushneryov O.S., Vida I.*

Abstract. Ensuring the cyber security management is an ever-increasing challenge for the financial institutions and the national financial regulators. The main purpose of the research is to improve cyber security management through analyzing large data volumes of information which helps to identify potential cyber threats at an early stage. The factors of the rapid cybercrime growth via supervised learning models with associated learning (SVM) were identified and evaluated in the paper. The object of research is 21 EU countries. The paper presents the results of an empirical analysis, which showed that the cyber threats are caused by the growth of using online banking (0.49), improvement of internet user skills (0.42), expansion of activities online (0.41). The results of the research can be useful for financial institutions, national regulators and cybersecurity professionals.

Key words: cybercrime, policy, financial system, big data, machine learning, innovation, sustainable development

DOI: 10.17512/pjms.2021.24.2.17

Article history:
Received August 30, 2021; *Revised* September 29, 2021*; Accepted* October 23, 2021

Introduction

Quarantine measures caused by the pandemic provoked an increase in payments on the Internet, an increase in the volume of electronic financial services, and the use of cryptocurrencies and altcoins as a means of payment and an investment instrument (Afonasova et al., 2019; Gyenge et al., 2021; Kobushko et al., 2021; Kostetskyi, 2021). These trends indicate an acceleration in the pace of digitalization of the economy and the transformation of approaches to organizing business processes (Költzsch, 2006). In these conditions, the digital transformation of financial relations opens up new opportunities for increasing the efficiency of financial institutions and reducing their costs by optimizing transactions, as well as a threat to their stable functioning - the spread of cyberattacks and an increase in the frequency of their implementation. In 2020, the damage from cybercrimes in the United States was estimated at $ 4.2 million, which is double that of 2018 ($ 2.7 million). At the same time, in recent years, financial services have been and remain the main target for cybercriminals. Based on data on attacks and incidents of information security

* **Jan Kubálek,** Ph.D. Department of Strategy, Faculty of Business Administration, Prague University of Economics and Business, Czech Republic. **Kuzmenko Olha** Prof., **Bozhenko Victoria** Assoc. Prof., **Kushneryov Olexandr** Assist**.,** Sumy State University, Ukraine.
Imre Vida, Hungarian University of Agriculture and Life Sciences, Doctoral School of Economics and Regional Sciences, Hungary
✉ corresponding author: info@vidaimre.
✉ kubalek@akkubalek.cz; info@vidaimre; o.kuzmenko@biem.sumdu.edu.ua

breaches from managed X-Force networks and publicly disclosed cybercrimes, IBM specialists established that the most vulnerable in 2020 were the spheres of finance, production, and energy.

In 2019, 39% of EU citizens who used the Internet faced security issues in the virtual space. The value of this indicator varies considerably in different member states: more than 50% in the UK and 10% in Lithuania (European Commission, 2020).

Dynamic digitalization of the economy makes banking and non-banking financial institutions more vulnerable to cybercrime (Lentner et al., 2019; Petroye et al., 2020). Financial institutions accumulate a significant amount of information from their customers (Ahmed et al., 2020). In case of the information security breach, confidential data may be used for illegal activities or sold on dark web sites, which may lead to the loss of business reputation of both financial institutions and their customers. (Brychko, Bilan, et al., 2021; Khrais, 2013; Plastun et al., 2018). In order to use personal data in commercial activities (banking, insurance, marketing, etc.) in the European Union in 2018 approved the General Data Protection Regulation (Limba et al., 2020; Teletov et al., 2020)

The growth of cyber attacks in the financial sector is the result of the rapid use of innovative digital technologies by financial institutions, the emergence of fintech companies (Petrushenko et al., 2018; Syniavska et al., 2019), and an increase in demand for digital financial products due to the COVID-19 pandemic (Serhiy Lyeonov, Bilan, et al., 2021; Kitukutha et al., 2021). In particular, during the pandemic, the number of cybersecurity violations among FinTech companies increased by an average of 17% (World Bank Group and the University of Cambridge, 2020).

Cybercrimes in the financial sector of the economy have reached an unprecedented scale, which is caused by the action of the following potential factors: an increase in the proportion of banking processes that are transferred to the management of third parties, including abroad (Pakhnenko et al., 2021); the use of cloud technologies for storing and transferring data (Paskevicius & Keliuotyte-Staniuleniene, 2018); increased use of robotics or algorithms for automated trading and application development (Stavrova, 2021); increased use of virtual and digital currencies.

Currently, cryptocurrency is used to legalize the proceeds of cybercrime (Humenna et al., 2020; Serhiy Leonov et al., 2019). In 2018, 4 billion pounds were legalized in Europe through cryptocurrencies. Cryptocurrency is inherently low-regulated and not controlled by a central authority, and therefore financial transactions cannot be closely monitored (Njegovanović, 2018).

Ensuring the security of information technologies of financial institutions and their databases is an ever-growing challenge for the top management of both financial institutions and the national regulator. (Gospodarchuk & Suchkova, 2019; Piontek, 2019; Skrynnyk & Vasylieva, 2020b).

One of the effective ways to improve the corporate management is the development and implementation of modern information and management systems and technologies (Strielkowski et al., 2017; Wierzbicka, 2018; Skrynnyk, 2021). The

practical implementation of information technology in business processes allows to obtain specific market advantages (Castro & Rebeca, 2014; Moradi, 2021; Vasilyeva et al., 2016; Skvarciany et al., 2021), improve the level of information security and create conditions for sustainable development (Chigrin & Pimonenko, 2014; Serhiy Lyeonov, Vasilyeva, et al., 2021).

Although the program is gradually becoming more secure, and developers are creating new approaches to cybersecurity, attackers are also improving malicious technologies. Traditional knowledge management technologies have limited capabilities to effectively detect and stop cyber threats (Yarovenko et al., 2021). New data management and analytic technologies help members of financial system become more proactive and intelligent and make better-informed security decisions Today, one of the main competitive advantages of the bank in the financial services market is the level of protection of personal data of customers and security of financial transactions (Bauk et al., 2017; Gaidelys & Valodkiene, 2011; Salciuviene et al., 2014).

Literature Review

Ensuring the cyber security management is an ever-increasing challenge for the financial institutions and the national financial regulators. Today, countering cyber threats is one of the main topics for discussion at international economic forums and conferences; this issue is widely covered in the works of foreign scientists.

To conduct a more thorough study of the definition of approaches to countering cyber threats in the financial sector, a bibliometric analysis was carried out using the VOSViewerv.1.6.10 toolkit, which allows identifying the relationships between objects, clustering, and visualizing scientometric data (Bilan, Pimonenko, et al., 2020). The object of bibliometric analysis was 3,328 scientific articles corresponding to the simultaneous inclusion in a search query of such categories as "cyber" and "financial" for the period 1993–2021 in publications indexed by the scientometric database Scopus. The study showed that the growth in the number of publications that deal with the study of information issues in the financial sector began with a rapid leap in 2013 and remains relevant to this day. In 2020, 328 publications on this topic were indexed by the scientometric database Scopus, which is 5.6 times more than in 2013. According to the results of the analysis of the frequency of use of keywords on this issue in scientific articles, three clusters were identified: cluster 1 – cybersecurity and its components (red on Fig. 1), cluster 2 – identification of cyber threats (green on Fig. 1), cluster 3 – Industry 4.0 concept and its impact on financial services (blue on Fig. 1).

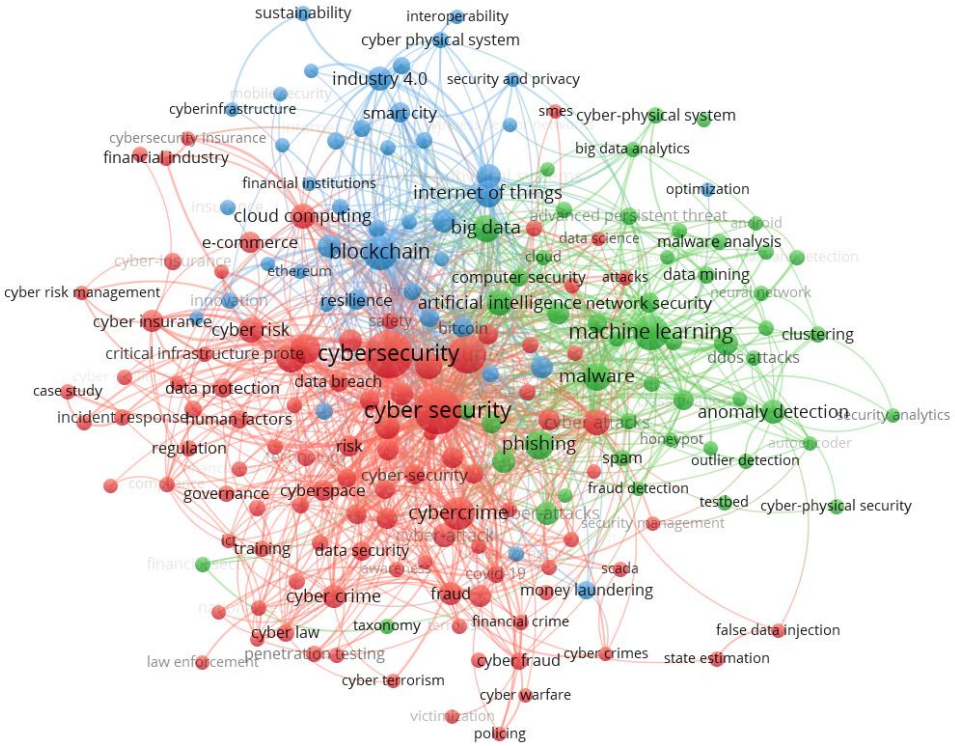

Figure 1: Results of bibliometric analysis of scientific papers on cyber security in the financial space for 1992–2021 in publications indexed by the scientometric Scopus database (VOSViewerv.1.6.10 toolkit)

Moreover, the analysis of international research centers engaged in the study of this issue, by geography, has been carried out. A third of publications on this topic (547 publications) were published by US scientists, while 10.6% of publications are from India, 8.5% – Great Britain, about 5% – Australia and China. These figures demonstrate that countering cyber threats remains a priority for any country globally, regardless of their level of economic development.

Within the framework of this study, we will analyze in more detail the publications of scientists within the framework of cluster 2, which deal with the analysis of methods for identifying and assessing cyber risks. The paper (Akhta et al., 2021) presents the results of a survey of chief information officers and chief information security officers, which made it possible to highlight the main challenges faced by small, medium, and large enterprises in the field of financial services in terms of data security and provision of appropriate protection tools and strategies.

Today, machine learning methods are being actively implemented in information protection and cybersecurity systems, which effectively solve the problems of analysis, classification, and forecasting of a broad class of data (Lopez et al., 2019;

Lopez & Alcaide, 2020). Al-Tahat and Moneim (2020) analyzed the areas of the practical application of neural networks, genetic algorithms, and an intelligent agent in the information security management system of commercial banks. The paper builds phase profiles of cyber fraudsters based on the analysis of their attack models using the technique of distributive semantics of natural language processing (Noor et al., 2019). Berdyugin and Revenkov (2020) developed software using Borland Delphi to quantify the probability of a cyberattack using e-banking technology.

The paper by Mousa et al. (2017) substantiates the need to strengthen information security among employees of financial institutions. Yerdon et al. (2021) proposed to use Eye-Tracking Active Indicators to identify cyber fraudsters from among employees of large companies.

One of the most common cyberattacks is phishing, which aims to steal confidential personal and financial information. Alhogail and Alsabih (2021) proposes a phishing email classifier model that applies deep learning algorithms using Graph Convolutional Network (GCN). Experimental tests confirmed that the classifier identified phishing lists with an accuracy of 98.2%.

The most common causes of malware infection and privacy violations are social networks (Onete et al., 2020; Kirichenko et al, 2017).

According to (Andreou & Anyfantaki, 2021; Leskaj, 2017; Serhiy Lyeonov & Liuta, 2016; Sági et al, 2020; Skrynnyk & Vasylieva, 2020a; Nuha et al., 2021; Vorontsova et al., 2021) of the rapid spread of cyber threats are low level of digital and financial literacy, the lack of public awareness of cyberattacks and their potential destructive consequences. In particular, Carlton et al. (2019) defines a set of cybersecurity skills of non-IT specialists that can reduce the risks of information security of the company.

Haddad (2021) analyzed the impact of artificial intelligence on the perfection of the accounting information system in commercial banks. Scientists (Arcuri et al., 2020; Kuzheliev et al., 2019; Tosun, 2021; Tweneboah-Koduah et al., 2020) **Błąd! Nie można odnaleźć źródła odwołania.**have estimated the impact of cyberattacks on the dynamics of changes in the price of shares of companies depending on their industry affiliation. Tweneboah-Koduah et al. (2020) has proved that cyberattacks on financial companies caused significant volatility in their stocks over time.

Based on the systematization of domestic and foreign scientific papers, it is established that to determine the relationship between parameters, as well as the degree and nature of the relationship between them in practice, various statistical and economic-mathematical methods and models are used: correlation (Didenko et al., 2020), avtoregressive (Bilan, Tiutiunyk, et al., 2020; Lyulyov et al., 2021), regression (Kobushko et al., 2021), neural models (Tetyana Vasilyeva et al., 2021), structural equations modeling (Brychko, Savchenko, et al., 2021), gravitation models (Serhiy Lyeonov et al., 2020) and comparative analysis (S. V. Leonov et al., 2012). Despite the large number of publications that deal with these issues, the scientific literature has not yet attempted to formalize the determinant of the spread of cyber fraud in the financial services sector.

Methodology

The main purpose of the research is to improve cyber security management through analyzing large data volumes of information that helps to identify potential cyber threats at an early stage. The paper proposes a scientific and methodological approach to formalizing the factors of the rapid spread of cyber fraud based on SVM machine learning methods.

Starting from the basic subject and issues as well as the research objectives of this study, there have been defined the following hypotheses:

H1: There is a significant correlation between online financial activities factors and cyberattacks.

H2: Digital skills factors have a significant influence on combating cyberattacks.

Testing the above hypotheses involves performing the following consequent steps:

1. Collection and processing of statistical data characterizing the volume of cybercriminal operations in the context of various cyberattack methods.

To reflect the intensity of cyberattacks in the context of European countries, the following indicators were used:

-share of mobiles infected with malware, % (I_1);
-share of users attacked by mobile banking trojans, % (I_2);
-users attacked by mobile ransomware trojans, % (I_3);
-share of users attacked by banking malware, % (I_4);
-share of users attacked by ransomware trojans, % (I_5);
-share of computers infected with at least one malware attack, % (I_6);
-share of computers facing at least one local malware attack, % (I_7);
-share of mobile users attacked via web sources, % (I_8);
-share of telnet attacks by originating country, % (I_9);
-share of attacks by cryptominers, % (I_{10});
-share of SSH-based attacks by originating country, % (I_{11});
-share of all Spam Emails by Originating Country (Yearly) (I_{12});
-share of countries targeted by malicious mailings, % (I_{13});
-share of computers attacked by phishing (yearly), % (I_{14}).

2. Bringing input indicators to a single comparable form. To standardize static indicators, the Z-normalization method was used, which provides for weighting the deviation of the actual level of each indicator from the average level for the set of countries under consideration to the standard deviation, according to the following formula:

$$k_{cj} = \frac{I_{cj} - \overline{I_J}}{\sigma_j} \quad (1)$$

where k_{cj} – the standardized value of the j-th indicator of the spread of cyber threats in the context of the c-th country;

I_{cj} – the actual value of the j-th indicator of the spread of cyber threats in the context of the c-th country;

$\overline{I_J}$ – arithmetic mean of the j-th indicator of the spread of cyber threats on the set of values of the considered set of countries;
σ_j – the average square deviation in the context of the j-th indicator of the spread of cyber threats on the set of values of the considered set of countries.
3. Aggregation of standardized levels of indicators of the spread of cyber threats to a single integral indicator. Analysis existing approaches to the construction of an integral indicator (S. V. Lyeonov et al., 2018; Vasylieva et al., 2020), the group method of data handling by Ivakhnenko is used, i.e., calculating the sum of the sums of squares of standardized values of input indicators as follows:

$$IK_c = \sum_{j=1}^{J} \sum_{j=1}^{J} \left(k_{cj}\right)^2 \quad ((2)$$

where IK_c – integral index of cyber threats in the context of the c-th country
Identification of potential factors influencing the spread of cyber fraud and collection of statistical data on them. To formalize the drivers of cybercrime spread, it is proposed to use the following variables: people who used the Internet to use online banking (Z1); mobile broadband index (Z2); Internet user skills (Z3); advanced skills and development (Z4); activities online (Z5); business digitisation (Z6).
4. Construction of the SVM machine learning model of two types (epsilon-SVM regression and nu-SVM regression) in the context of four reference vector specifications: linear, polynomial, radial basis functions (RBF), and sigmoid.
In regression, it is necessary to estimate the functional dependence of the dependent variable y on the set of independent variables x. It provides, like other regression problems, that the relationship between the independent and dependent variables is given by a deterministic function f, taking into account some additive noise:

$$y = f(x) + noise \quad (3)$$

SVM regression type 1. For this type SVM model:

$$\frac{1}{2} w^T w + C \sum_{i=1}^{N} \xi_i + C \sum_{i=1}^{N} \xi_i^* \rightarrow min \quad (4)$$

$$\begin{cases} w^T \phi(x_i) + b_i - y_i \leq \varepsilon + \xi_i^* \\ y_i - w^T \phi(x_i) - b_i \leq \varepsilon + \xi_i \\ \xi_i^*, \xi_i \geq 0, i = 1, \dots, N \end{cases}$$

where C – the capacitance parameter (used for grid cross-validation).
SVM regression type 2. For this type SVM model:

$$\frac{1}{2} w^T w - C \left(v\varepsilon + \frac{1}{N} \sum_{i=1}^{N} (\xi_i + \xi_i^*) \right) \rightarrow min \quad (5)$$

$$\begin{cases} w^T \phi(x_i) + b_i - y_i \leq \varepsilon + \xi_i \\ y_i - w^T \phi(x_i) - b_i \leq \varepsilon + \xi_i^* \\ \xi_i^*, \xi_i \geq 0, i = 1, \dots, N, \varepsilon \geq 0 \end{cases}$$

Using the reference vector method, it is possible to construct various types of functional dependencies between variables (linear, polynomial, radial basis, sigmoid):

$$\phi = \begin{Bmatrix} x_i \cdot x_j \quad Linear \\ \left(\gamma x_i \cdot x_j + coefficient\right)^d \quad Polynomial \\ exp\left(-\gamma\left(x_i - x_j\right)^2\right) \quad RBF \\ tanh\left(\gamma x_i \cdot x_j + coefficient\right) \quad Sigmoid \end{Bmatrix} \tag{6}$$

where d – the degree of the polynomial kernel;
γ – gamma parameter for polynomial, RBF and sigmoid nuclei;
$coefficient$ – coefficient for polynomial and sigmoid nuclei;
21 European countries were selected as the object of the research. The source of primary information was data from Comparitech (2020), European Commision. (2020). Statistica software package for statistical analysis was used to carry out mathematical calculations.

Results

Ensuring the security of information technologies of financial institutions and their databases is an ever-growing challenge for the top management of both financial institutions and the national regulator. Although the program is gradually becoming more secure, and developers are creating new approaches to cybersecurity, attackers are also improving malicious technologies. To counter cyber threats in the economy's financial sector, it is advisable to identify trigger factors leading to an increase in cyber fraud in financial services.
Systematized data on cases of cyber fraud in the context of various methods of their implementation using data from Comparitech (2020) are presented in the Table 1.

Table 1. Information on the state of cybercrime in European countries as of 2020

	Top 3 countries			Bottom 3 countries		
	1	2	3	1	2	3
% of Mobiles Infected with Malware (I_1)	Romania (5,04%)	Spain (4,31%)	Slovakia (3,5%)	Finland (1,06%)	Denmark (1,33%)	Germany (1,63%)
% Share of Users Attacked by Banking Malware (I_4)	Portugal (0,9%)	Greece (0,5%)	Bulgaria (0,5%)	Ireland (0,1%)	Denmark (0,1%)	Hungary (0,2%)
% of Attacks by Cryptominers (I_{10})	Latvia (0,73%)	Bulgaria (0,56%)	Slovakia (0,5%)	Denmark (0,11%)	Germany (0,12%)	Romania (0,14%)
% of all Spam Emails by Originating Country (I_{12})	Germany (10,97%)	France (5,97%)	Netherlands (4,00%)	Denmark (0,07%)	Slovakia (0,19%)	Sweden (0,19%)
% of Computers Attacked by Phishing (Yearly) (I_{14})	Portugal (19,73%)	France (17,9%)	Belgium (16,4%)	Denmark (3,26%)	Sweden (3,35%)	Ireland (3,42%)

Based on the types of cyberattacks analyzed in Table 1, we note that the largest victim countries in 2020 were Spain, Portugal, and Latvia, while the lowest number

of cyberattacks was recorded in countries such as Denmark, Sweden, and Ireland. In particular, 19.73% of computers in Portugal were attacked by Internet scams such as phishing, while in Denmark, it was only 3.26%. The shift to telecommuting and the intensive use of e-services caused by the COVID-19 pandemic has led to an increase in cyber fraud worldwide. As for the European countries, the largest number of detected malicious files associated with the Covid-19 pandemics were found in Spain, Italy, and Germany.

The existing array of statistical data was standardized based on the Z-normalization method (formula 1), which made it possible to aggregate into a single generalizing indicator – the cyber threat index. The results of calculating the cyber threat index using Formula (2) are shown in Figure 2.

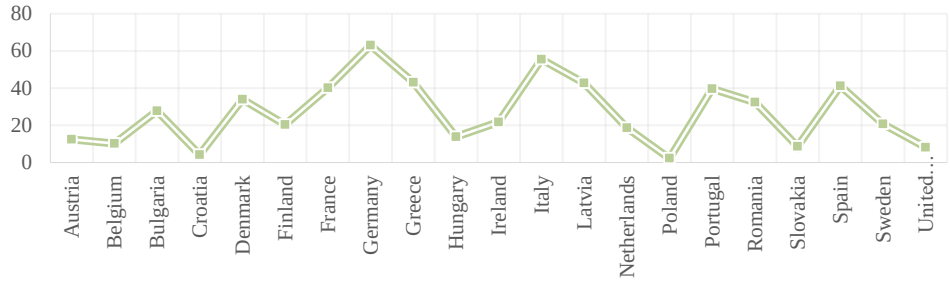

Figure 2: Dynamics of the cyber threat index in European countries in 2020

The calculations demonstrated the unevenness of the implementation of cyberattacks in the context of European countries since the cyber threat index in 2020 varies from 2.4 conventional units up to 74.9 conventional units Based on the aggregation of 15 input indicators characterizing various ways of carrying out fraud in the information space, it was found that the highest level of cyber threats in 2020 was observed in countries such as Spain (74.9 conventional units), Germany (63.3 conventional units), Italy (57.7 conventional units), Latvia (42.9 conventional units), and France (40.2 conventional units).

The next stage of the proposed scientific and methodological approach is to determine the determinants of the spread of cyber threats by building 8 SVM machine learning models: two types (epsilon-SVM regression and nu-SVM regression) in the context of four specifications of reference vectors: linear, polynomial, radial basis functions (RBF) and sigmoid. Based on comparing the actual and predicted levels of the cybersecurity spread determinants and the cyberthreat index for the test sample of countries, we calculate the standard deviation (Table 2).

Table 2. Comparison of 8 built SVM models

	Denmark	Italy	Latvia	Netherlands	Slovakia	Spain	Standard deviation
Cyberthreat Index	63,33	57,71	42,91	18,81	8,90	74,92	
Epsilon-SVM regression: Linear	23,92	32,11	9,87	36,23	19,74	32,50	21,15
Epsilon-SVM regression: Polynomial	24,08	26,02	25,38	17,44	25,21	24,81	20,69
Epsilon-SVM regression: Radial	17,09	27,93	19,68	23,59	21,38	22,23	21,24
Epsilon-SVM regression: Sigmoid	27,69	32,03	22,62	21,15	24,34	29,82	20,15
Nu-SVM regression 2: Linear	33,39	42,77	21,84	16,20	25,87	27,74	20,51
Nu-SVM regression 2: Polynomial	26,03	26,03	25,98	15,91	25,39	24,52	20,71
Nu-SVM regression 2: Radial	29,48	37,48	28,72	16,45	28,24	24,30	20,20
Nu-SVM regression 2: Sigmoid	27,84	33,34	28,04	19,77	27,46	25,30	**20,00**

Thus, the sigmoid nu-SVM regression model is the most accurate for determining the determinants of the spread of cyber threats. This model has the following characteristics: the number of independent variables in the model is 6, the model type is nu-SVM regression, the Kernel type is sigmoid, the number of reference vectors that allow the pattern recognition algorithm is 9, among which the boundary ones are 3 (Table 3).

Table 3. SVM model specification for determining the determinants of cyber threats spread

	Weights	Banking	Mobile broadband	Internet User Skills	Advanced Skills and Development	Activities online	Business digitisation
1	-9,9177	0,8050	0,0624	0,6413	0,3470	0,4146	0,7958
2	-10,0000	0,5653	0,0524	0,5627	0,3730	0,5692	0,3235
3	9,2885	0,9800	0,5878	0,8980	0,4980	0,8886	0,7657
4	9,2038	0,7392	0,4457	0,5712	0,3063	0,0000	0,4487
5	10,0000	0,3456	0,0373	0,4235	0,0000	0,4438	0,2369
6	-1,8307	0,5576	0,6584	0,3970	0,2656	0,5710	0,0210
7	-10,0000	0,5655	0,3311	0,2987	0,1942	0,2245	0,0762
8	9,0077	0,5286	0,0902	0,5133	0,0241	0,4212	0,3393
9	-5,7516	0,8343	0,3410	0,9606	0,5029	0,8230	0,6473

Based on the results of the calculations, we note the following: among the 9 constructed reference vectors, vectors 2, 5, and 7 have the most significant weight in

absolute value. Thus, to determine the determinants of the spread of cyber threats, in the context of each reference vector, we will calculate the arithmetic mean value for the three selected reference vectors. Thus, we get the following ranking of the importance of the determinants of the spread of cyber threats:
Thus, having built a neural model using the reference vector machine based on data from the European Union countries, we found a strong functional relationship between the level of cyber threats and factors such as the proportion of the population using online banking (0.49), an indicator of the level of skills on the Internet (0.42), and an indicator of online activity (0.41).

Conclusion

Financial market participants need confidence in data security, the ability to minimize cyber risks and defend against cyber threats. Increasing financial damage from cyberattacks, combined with the growing volume of information data stored in the network infrastructure necessitate the development of new tools to ensure information security. To combat cybercrime, a combination of traditional and non-traditional strategies and tactics using digital information technology. To make managerial decisions in the field of cybersecurity, the development of tools is gaining ground, which involves the accumulation of large amounts of information and the use of modern approaches in the field of artificial intelligence. Having built a neural model using the reference vector machine based on data from the European Union countries, we found a strong functional relationship between the level of cyber threats and factors such as the proportion of the population using online banking (0.49), an indicator of the level of skills on the Internet (0.42), and an indicator of online activity (0.41). An important step in the cybersecurity system is the timely identification of cyber threats and taking rapid action to neutralize them. In the conditions of constantly growing cyber risks it is expedient to create conditions for ensuring cyber resilience by strengthening the control of the level of banking and financial operations performed without the consent of clients; training of employees responsible for information protection and response to cyber threats; informing employees who are not involved in the organization of cybersecurity, as well as bank customers; use the technology of cryptographic information protection

Acknowledgement

This research was funded by the grant from the Ministry of Education and Science of Ukraine (No. s/r 0121U100467, 0121U109559, 0120U100473). Supported by the ÚNKP-21-3. New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

References

Ahmed, R. R., Romeika, G., Kauliene, R., Streimikis, J. and Dapkus, R., (2020). ES-QUAL model and customer satisfaction in online banking: Evidence from multivariate analysis techniques. *Oeconomia Copernicana*, *11*(1).

Afonasova, M. A., Panfilova, E. E., Galichkina, M. A. and Ślusarczyk, B., (2019). Digitalization in economy and innovation: The effect on social and economic processes. *Polish Journal of Management Studies*.

Akhta, S., Sheorey, P. A., Bhattacharya, S. and Ajith, K. V. V., (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research*, *12*(1).

Al-Tahat, S., Moneim, O. A., (2020). The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks. *International Journal of Scientific and Technology Research*, *9*(3).

Alhogail, A., Alsabih, A., (2021). Applying machine learning and natural language processing to detect phishing email. *Computers and Security*, *110*.

Andreou, P. C., Anyfantaki, S., (2021). Financial literacy and its influence on internet banking behavior. *European Management Journal*, *39*(5).

Arcuri, M. C., Gai, L., Ielasi, F. and Ventisette, E., (2020). Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2).

Bauk, S., Kapidani, N. and Schmeink, A., (2017). On intelligent use of ICT in some maritime business organizations. *Montenegrin Journal of Economics*, *13*(2).

Berdyugin, A. A., Revenkov, P. V., (2020). Cyberattack risk assessment in electronic banking technologies (the case of software implementation). *Finance: Theory and Practice*, *24*(6).

Bilan, Y., Pimonenko, T. and Starchenko, L., (2020). Sustainable business models for innovation and success: Bibliometric analysis. *E3S Web of Conferences*, *159*.

Bilan, Y., Tiutiunyk, I., Lyeonov, S. and Vasylieva, T., (2020). Shadow economy and economic development: A panel cointegration and causality analysis. *International Journal of Economic Policy in Emerging Economies*, *13*(2).

Brychko, M., Bilan, Y., Lyeonov, S. and Mentel, G., (2021). Trust crisis in the financial sector and macroeconomic stability: a structural equation modelling approach. *Economic Research-Ekonomska Istrazivanja* , *34*(1).

Brychko, M., Savchenko, T., Vasylieva, T. and Piotrowski, P., (2021). Illegal activities of financial intermediaries: A burden of trust crisis. *Journal of International Studies*, *14*(1).

Carlton, M., Levy, Y. and Ramim, M., (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer*

Castro, E. L., Rebeca, M., (2014). Decision making in the financial management of the business enterprise. *Journal of Intercultural Management*, *5*(2).

Chigrin, O., Pimonenko, T., (2014). The ways of corporate sector firms financing for sustainability of performance. *International Journal of Ecology and Development*, *29*(3).

Didenko, I., Paucz-Olszewska, J., Lyeonov, S., Ostrowska-Dankiewicz, A. and Ciekanowski, Z., (2020). Social safety and behavioral aspects of populations financial inclusion: A multicountry analysis. *Journal of International Studies*, *13*(2).

Gaidelys, V., Valodkiene, G., (2011). The methods of selecting and assessing potential consumers used of by competitive intelligence. *Engineering Economics*, *22*(2).

Gospodarchuk, G., Suchkova, . E., (2019). Financial stability: problems of inter-level and cross-sectoral equilibrium. Equilibrium. *Quarterly Journal of Economics and Economic Policy*, 14(1), 53–79.

Gyenge, B., Máté, Z., Vida, I., Bilan, Y. and Vasa, L., (2021). A New Strategic Marketing Management Model for the Specificities of E-Commerce in the Supply Chain. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(4), 1136-1149.

Haddad, H., (2021). The effect of artificial intelligence on the AIS excellence in Jordanian banks. *Montenegrin Journal of Economics*, *17*(4).

Humenna, Y., Lyeonov, S., Tiutiunyk, I., Bilan, Y., Srovnalíková, I. P. and Streimikis, J., (2020). From shadow economy to lower carbon intensity: theory and evidence. *International Journal of Global Environmental Issues*, *19*(1/2/3).

Khrais, L., (2013). The effectiveness of e-banking environment in customer life service an empircal study (Poland). *The Effectiveness of E-Banking Environment in Customer Life Service an Empircal Study (Poland)*, *8*(1).

Kitukutha, N.M., Vasa, L. and Oláh, J., (2021). The impact of COVID-19 on the economy and sustainable e-commerce. *Forum Scientiae Oeconomia 9*(2), 47-72.

Kobushko, I., Tiutiunyk, I., Kobushko, I., Starinskyi, M. and Zavalna, Z., (2021). The triadic approach to cash management: Communication, advocacy, and legal aspects. *Estudios de Economia Aplicada*, *39*(7).

Költzsch, G., (2006). Innovative methods to enhance transaction security of banking applications. *Journal of Business Economics and Management*, *7*(4).

Kuzheliev, M., Rekunenko, I., Boldova, A., Zhytar, M. and Stabias, S., (2019). Modeling of structural and temporal characteristics in the corporate securities market of Ukraine. *Investment Management and Financial Innovations*, *16*(2).

Lentner, Cs., Vasa, L., Kolozsi, P.P. and Zéman, Z., (2019). New dimensions of internal controls in banking after the GFC. *Economic Annals-XXI 176*(3-4), 38-48.

Leonov, Serhiy, Yarovenko, H., Boiko, A. and Dotsenko, T., (2019). Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings*, *2422*, 297–307.

Leonov, S. V., Vasylieva, T. A. and Tsyganyuk, D. L., (2012). Formalization of functional limitations in functioning of co-investment funds basing on comparative analysis of financial markets within FM CEEC. *Actual Problems of Economics*, *134*(8).

Leskaj, E., (2017). The Challenges Faced by the Strategic Management of Public Organizations. *Administratie Si Management Public*, *29*.

Limba, T., Driaunys, K., Kiskis, M. and Sidlauskas, A., (2020). Development of digital contents: Privacy policy model under the general data protection regulation and user-friendly interface. *Transformations in Business and Economics*, *19*(1).

Lopez, B. S., Alcaide, A. V., (2020). Blockchain, Artificial Intelligence, Internet of Things to Improve Governance, Financial Management and Control of Crisis: Case Study COVID-19. *SocioEconomic Challenges*, *4*(2).

Lopez, B. S., García, D. I. and Alcaide, A. V., (2019). Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges*, *3*(4).

Lyeonov, Serhiy, Bilan, S., Yarovenko, H., Ostasz, G. and Kolotilina, O., (2021). Country's health profile: Social, economic, behavioral and healthcare determinants. *Economics and Sociology*, *14*(3).

Lyeonov, Serhiy and Liuta, O., (2016). Actual problems of finance teaching in Ukraine in

the post-crisis period. In *The Financial Crisis: Implications for Research and Teaching* (pp. 145–152). Springer International Publishing.

Lyeonov, Serhiy, Vasilyeva, T., Bilan, Y. and Bagmet, K., (2021). Convergence of the institutional quality of the social sector: The path to inclusive growth. *International Journal of Trade and Global Markets*, *14*(3).

Lyeonov, Serhiy, Żurakowska-Sawa, J., Kuzmenko, O. and Koibichuk, V., (2020). Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies*, *13*(4).

Lyeonov, S. V., Vasylieva, T. A. and Lyulyov, O. V., (2018). Macroeconomic stability evaluation in countries of lower-middle income economies. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, *1*.

Lyulyov, O., Paliienko, M., Prasol, L., Vasylieva, T., Kubatko, O. and Kubatko, V., (2021). Determinants of shadow economy in transition countries: Economic and environmental aspects. *International Journal of Global Energy Issues*, *43*(2–3).

Moradi, M., (2021). Importance of Internet of Things (IoT) in Marketing Research and Its Ethical and Data Privacy Challenges. *Business Ethics and Leadership*, *5*(1).

Mousa, M., Sai, A. A. and Salhin, G., (2017). An Exploration for the Motives behind Enhancing Senior Banker's Level of Organizational Resilience: A Holistic Case Study. *Journal of Intercultural Management*, *9*(4).

Noor, U., Anwar, Z., Amjad, T. and Choo, K. K. R., (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, *96*.

Nuha, M., Mahmud, S. and Sattar, A., (2021). A Case Study and Fraud Rate Prediction in e-Banking Systems Using Machine Learning and Data Mining. *Advances in Intelligent Systems and Computing*, *1248*.

Onete, C. B., Vargas, V. M. and Chita, S. D., (2020). Study on the implications of personal data exposure on the social media platforms. *Transformations in Business and Economics*, *19*(2).

Pakhnenko, O., Rubanov, P., Hacar, D. and Yatsenko, V., (2021). Digitalization of financial services in European countries: Evaluation and comparative analysis. *Journal of International Studies*, *14*(2).

Petroye, O., Lyulyov, O., Lytvynchuk, I., Paida, Y. and Pakhomov, V., (2020). Effects of Information Security and Innovations on Country's Image: Governance Aspect. *International Journal of Safety and Security Engineering*, *10*(4).

Petrushenko, Y., Kozarezenko, L., Glinska-Newes, A., Tokarenko, M. and But, M., (2018). The opportunities of engaging FinTech companies into the system of crossborder money transfers in Ukraine. *Investment Management and Financial Innovations*, *15*(4).

Piontek, B., (2019). The theoretical basis of strategic security management for shaping the structural order and sustainability processes. *Polish Journal of Management Studies*, *20*(1).

Plastun, A., Makarenko, I., Yelnikova, Y. and Sheliuk, A., (2018). Crisis and financial data properties: A persistence view. *Journal of International Studies*, *11*(3).

Sági, J., Vasa, L. and Lentner, Cs., (2020). Innovative Solutions in the Development of Households' Financial Awareness: A Hungarian Example. *Economics & Sociology 13* (3), 27-45.

Salciuviene, L., Auruskeviciene, V. and Ivanauskiene, N., (2014). Key Drivers Affecting Customer Intention to Purchase Financial Services Online. *Engineering Economics*,

25(2).
Skvarciany, V., Jurevičienė, D., Iljins, J. and Gaile-Sarkane, E., (2018). Factors influencing a bank's competitive ability: the case of Lithuania and Latvia. *Oeconomia Copernicana*, *9*(1), 7–28.
Strielkowski, W., Gryshova, I. and Kalyugina, S., (2017). Modern technologies in public administration management: A comparison of Estonia, India and United Kingdom. *Administratie Si Management Public*. (28), 174-185
Syniavska, O., Dekhtyar, N., Deyneka, O., Zhukova, T. and Syniavska, O., (2019). Modeling the process of counteracting fraud in e-banking. *CEUR Workshop Proceedings*, *2422*.
Teletov, A., Teletova, S., Letunovska, N. and Lazorenko, V., (2020). Innovations in online advertising management of ukrainian business entities. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1 Special Issue 2).
Tosun, O. K., (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*.
Tweneboah-Koduah, S., Atsu, F. and Prasad, R., (2020). Reaction of stock volatility to data breach: An event study. *Journal of Cyber Security and Mobility*, *9*(3).
Vasilyeva, T., Sysoyeva, L. and Vysochyna, A., (2016). Formalization of factors that are affecting stability of Ukraine banking system. *Risk Governance and Control: Financial Markets and Institutions*, *6*(4), 7–11.
Vasilyeva, T., Kuzmenko, O., Kuryłowicz, M. and Letunovska, N., (2021). Neural network modeling of the economic and social development trajectory transformation due to quarantine restrictions during covid-19. *Economics and Sociology*, *14*(2).
Vasylieva, T., Jurgilewicz, O., Poliakh, S., Tvaronavičienė, M. and Hydzik, P., (2020). Problems of measuring country's financial security. *Journal of International Studies*, *13*(2), 329–346.
Vorontsova, A., Vasylieva, T., Lyeonov, S., Artyukhov, A. and Mayboroda, T., (2021). Education Expenditures as a Factor in Bridging the Gap at the Level of Digitalization. *2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 - Proceedings*.
Wierzbicka, W., (2018). Information infrastructure as a pillar of the knowledge-based economy — an analysis of regional differentiation in Poland. *Equilibrium*, *13*(1).
Yarovenko, H., Bilan, Y., Lyeonov, S. and Mentel, G., (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management*, *22*(2).
Yerdon, V. A., Lin, J., Wohleber, R. W., Matthews, G., Reinerman-Jones, L. and Hancock, P. A., (2021). Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management*.

PODEJŚCIE DO ZARZĄDZANIA INNOWACJAMI W CELU OCHRONY SEKTORA FINANSOWEGO PRZED CYBERPRZESTĘPCZOŚCIĄ

Streszczenie. Zapewnienie zarządzania cyberbezpieczeństwem jest coraz większym wyzwaniem dla instytucji finansowych i krajowych organów nadzoru finansowego. Głównym celem badania jest usprawnienie zarządzania cyberbezpieczeństwem poprzez analizę dużych wolumenów danych informacji, co pomaga zidentyfikować potencjalne zagrożenia cybernetyczne na wczesnym etapie. W artykule zidentyfikowano i oceniono

czynniki szybkiego wzrostu cyberprzestępczości poprzez nadzorowane modele uczenia się z powiązanym uczeniem (SVM). Przedmiotem badań jest 21 krajów UE. W artykule przedstawiono wyniki analizy empirycznej, która wykazała, że cyberzagrożenia spowodowane są wzrostem korzystania z bankowości internetowej (0,49), poprawą umiejętności internautów (0,42), ekspansją aktywności w sieci (0,41). Wyniki badania mogą być przydatne dla instytucji finansowych, krajowych regulatorów i specjalistów ds. cyberbezpieczeństwa.

Słowa kluczowe: cyberprzestępczość, polityka, system finansowy, big data, uczenie maszynowe, innowacje, zrównoważony rozwój

管理创新以保护金融部门免遭网络犯罪的方法

抽象的。确保网络安全管理是金融机构和国家金融监管机构面临的日益严峻的挑战。该研究的主要目的是通过分析大量信息数据来改善网络安全管理，这有助于在早期识别潜在的网络威胁。该论文通过具有关联学习 (SVM) **的**监督学习模型确定并评估了网络犯罪快速增长的因素。研究对象为欧盟21**个国家。本文提出了**实证分**析的**结果，表明网络威胁是由使用网上银行的增长 (0.49)、**互**联网用户技能的提高 (0.42) **和在**线活动的扩展 (0.41) **引起的。研究**结果可能对金融机构、国家监管机构和网络安全专业人士有用。

关键词：网络犯罪，政策，金融体系，大数据，机器学习，创新，可持续发展