МУКАЧІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

НАУКОВИЙ ВІСНИК ЕКОНОМІКА

Випуск 8, № 1. С. 144–153
URL: https://economics-msu.com.ua/en

УДК 330.46:336.71:343.37]:004.056.5
DOI: 10.52566/msu-econ.8(1).2021.144-153

Економіко-математичне моделювання ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів аналізу виживання

Ольга Віталіївна Кузьменко[1], Тетяна Віталіївна Доценко[2], Лілія Олегівна Скринька[1]

[1]Сумський державний університет
40007, вул. Римського-Корсакова, 2, м. Суми, Україна

[2]ТВБВ №10018/0172 філії – Сумського обласного управління АТ «Ощадбанк»
40016, вул. Катерини Зеленко, 4, м. Суми, Україна

Анотація. У сучасному світі цифровізація фінансових відносин, розвиток інноваційних технологій, поява та використання криптовалют для розрахунків зумовлюють зростання кількості кібершахрайств у фінансовій сфері та їх інтелектуалізації, збільшення нелегального відтоку коштів за кордон. Неефективні рішення та бездіяльність у протидії даним загрозам призводить до масштабних негативних наслідків як фінансового, так і суспільного характеру. Метою даного дослідження є реалізація економіко-математичного моделювання ефективності національної системи протидії кібершахрайствам і легалізації кримінальних доходів, в основі якого лежить використання методів аналізу виживання. У статті проведено бібліометричний аналіз публікацій, присвячених проблемі ефективності кібершахрайств та протидії легалізації незаконних коштів, за допомогою побудови бібліометричної карти ключових слів, з використанням програмного забезпечення VOSviewer. Це дозволило виділити 7 кластерів основоположних категорій аналізу кібершахрайств. А зміни векторів досліджень науковців показала візуалізаційна карта контекстуально-часового виміру досліджень ефективності кібершахрайств у виданнях бази даних Scopus. У роботі досліджено ефективність національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі таблиць виживання. У результаті дослідження було здійснено аналіз ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методу Каплана-Мейєра. Виявлено залежності ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів від часового інтервалу після виявлення фактів порушення. Практична цінність застосування розробленої моделі полягає у формуванні аналітичного підґрунтя щодо подальшого прийняття управлінських рішень Національним банком України, Державною службою фінансового моніторингу, Службою безпеки України в розрізі ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів та необхідності її коригування

Ключові слова: банки, кібершахрайство, легалізація кримінальних доходів, метод Каплана-Мейєра, національна система протидії відмиванню коштів

Стаття надійшла: 20.12.2020, Доопрацьовано: 18.02.2021, Схвалено до друку: 20.03.2021

MUKACHEVO STATE UNIVERSITY

SCIENTIFIC BULLETIN ECONOMICS

Volume 8, No. 1, 144-153
Journal homepage: https://economics-msu.com.ua/en

Economic and Mathematical Modelling of the Effectiveness of the National System for Countering Cyber Fraud and Criminal Proceeds Legalisation Based on Survival Analysis Methods

Olha V. Kuzmenko[1]*, Tetiana V. Dotsenko[2], Liliia O. Skrynka[1]

[1]Sumy State University
40007, 2 Rymskyi-Korsakov Str., Sumy, Ukraine

[2]Territorially Autonomous Non-Accounting Branch No. 10018/0172
of the Branch – Sumy Regional Department of Oschadbank JSC, Ukraine
40016, 4 Kateryna Zelenko Str., Sumy, Ukraine

Abstract. In the modern world, the digitalisation of financial relations, the development of innovative technologies, the emergence and use of cryptocurrencies for payments lead to an increase in the number of cyber fraud in the financial sector and their intellectualisation, an increase in the illegal outflow of funds abroad. Ineffective decisions and inaction in countering these threats lead to large-scale negative consequences, both financial and public. The purpose of this study is to carry out economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation, which is based on the use of survival analysis methods. This study provides a bibliometric analysis of research papers devoted to the problem of cyber fraud efficiency and countering the legalisation of illegal funds by building a bibliometric keyword map using VOSviewer software. This allowed identifying 7 clusters of fundamental categories of cyber fraud analysis. And changes in the research vectors of researchers were shown by the visualisation map of the contextual and temporal dimension of papers on the cyber fraud efficiency in publications of the Scopus database. The study examines the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on survival tables. As a result of the study, the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation was analysed based on the Kaplan-Meyer method. The effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation depends on the time interval after the detection of violations. The practical significance of applying the developed model is to form an analytical basis for further management decision-making by the National Bank of Ukraine, the State Financial Monitoring Service, and the Security Service of Ukraine in the context of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation and the need to adjust it

Keywords: banks, cyber fraud, money laundering, Kaplan-Meyer method, national anti-money laundering system

Received: 20.12.2020, Revised: 18.02.2021, Accepted: 20.03.2021

Suggested Citation: Kuzmenko, O.V., Dotsenko, T.V., & Skrynka, L.O. (2021). Economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on survival analysis methods. *Scientific Bulletin of Mukachevo State University. Series "Economics"*, 8(1), 144-153.

*Corresponding author

Introduction

Cyber fraud and the legalisation of proceeds from crime pose a threat to the economic security of any country, and it becomes global in nature, since various money laundering schemes are essentially international and contain a link with organised crime. That is why the development of modern economic science is impossible within the isolated territory of a particular country. An analytical understanding of the current state and effectiveness of ensuring the national anti-money laundering system is important. Such information is necessary for political figures, state regulatory and law enforcement agencies, economic agents, financial institutions and organisations, business entities, individuals to determine the priority of problems in this area and make a decision on the appropriate adoption of adequate measures to resolve important aspects of countering the illegal circulation of funds [1; 2].

For its part, shortcomings in the legislation on the legalisation of criminal proceeds, lack of targeted attention to the legality of assets, insufficient experience in financial and economic investigations of fraudulent money laundering, imperfect and incomplete reporting structure in the direction of the legality of funds rotation, strengthen the relevance of the issue of eliminating key gaps in the national system of countering cyber fraud and money laundering, by combining existing mechanisms with specialised methods of data analysis on the risks and consequences of fraudulent money laundering [3]. Thus, knowledge and awareness of the specifics and forecasts in the direction of countering money laundering based on specific modelling methods would make a significant contribution to preventing the legalisation of illegal income both at the national and international levels.

At the same time, special attention should be paid to modelling based on methods of survival analysis, which is a type of statistical modelling that allows assessing and analysing the probability of occurrence of certain consequences over time. Data modelled by this method must be prepared in a certain way for analysis in a censored (incomplete) form, that is, the desired dependent variable characterises the occurrence of a probable consequence in time, provided that the time lag is limited.

The purpose of the study consists in developing a structural and logical model for evaluating the effectiveness of the national system for countering cyber fraud and legalising criminal proceeds.

Research objectives are: to conduct a bibliometric analysis of research papers related to the concept of cyber fraud effectiveness and countering the legalisation of funds obtained by criminal means, using the construction of a bibliometric map of keywords; to analyse the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on the Kaplan-Meyer method; to identify the dependence of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation on the time interval after the detection of violations.

Literature Review

Taking into account the literature sources, it is worth noting that general theoretical and practical issues of countering the legalisation of criminal proceeds obtained illegally are revealed by many Ukrainian and foreign scientists. Thus, L. De Koker, T.T.H. Tran [1] describe the opposition to the legalisation of illegal income in Vietnam through the improvement of the legal framework for the confiscation of proceeds from crime. O. Lebid, O. Veits [2] search for statistically approved criteria and attributes to identify the risk of illegal money laundering. M. Levi [3] assesses control over money laundering; V. Vovk, Yu. Zhezherun, O. Bilovodska, V. Babenko, A. Biriukova [4] reveal the managerial and legal aspects of financial monitoring in the bank as a market instrument in the context of innovative development and digitalisation of the economy. For its part, the problem of countering cyber fraud is addressed in the treatises of modern researchers, including Chen, Y. Yuan, H. (Robert) Luo, J. Jian, Y. Wang [5] regarding the identification of group transnational assets of cyber fraud. I. Kara, M. Aydos [6] investigate cyber fraud through the detection and analysis of cryptocurrency software. S. Kemp, F. Miro-Llinares, A. Moneva [7] study the growth of cyber fraud in Europe. L.M. Lux, G.O. Calderon [8] define and differentiate types of cyber fraud.

It is worth noting that modelling of existing and projected systems and processes is widely used to analyse various issues in all sectors of the world and national economy today. For example, the gravitational model is used by J. Ferwerda, A. van Saase, B. Unger, M. Getzner [9] for estimating money laundering flows; probabilistic approach – T.I. Safronova, S.A. Vladimirov, I.A. Prikhodko [10], offer mathematical modelling of technological processes of optimisation of the use of resources; factor financial analysis – A. Borodin, I. Mityushina, E. Streltsova, A. Kulikov, I. Yakovenko and A. Namitulina [11] which is used to model the prospects for the development of an enterprise; Matrix modelling is described by Wubneh, F.M. Desta, H.A. Kahsay [12]; other models. Among such models, a specific method of economic and mathematical modelling is the modelling based on methods of survival analysis, which is covered by the following specialists: Shoaee, E. Khorram [13] – general theoretical features are investigated; K. Platero, M.S. Tobar [14] and N. Stevens, M. Lydon, A.H. Marshall, S. Taylor [15] – practical application in the field of Medicine and healthcare

is described. Although a fairly significant circle of modern researchers around the world is studying the effectiveness of the national system for countering the legalisation of criminal proceeds, as well as combating cyber fraud, this issue remains open and requires significantly more new developments and acquisitions.

Materials and Methods

Initially, a bibliometric analysis of research papers for 2010-2020 was carried out. A map of the relationship between the concept of "cyber fraud efficiency" and other scientific categories was formed. VOSviewer was the tool for implementing this map. Direct economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and money laundering was carried out through a number of stages, each of which used appropriate methodological tools.

Stage 1 – ***Establishment of the input data base of the study***. For the implementation of the study, 70 Ukrainian banks were selected for 2019, which were declared insolvent by the National Bank of Ukraine with further dissolution. The corresponding dates in the format: month, date, year are shown in columns 1-6 of Table 1. To characterise the national system of countering cyber fraud and criminal proceeds legalisation, 9 indicators were selected in the context of the 70 banks of Ukraine (columns 7-11 of Table 1): *K1* – share of financial transactions registered based on the internal financial monitoring; *K2* – the ratio of the amount of commission income from cash settlement services to the total number of bank customers; *K3* – violation of the NBU state of emergency; *K4* – violation of the Law of Ukraine "on legalisation"; *K5* – violation of the Law of Ukraine "on banks"; *K6* – the ratio of the number of clients who did not perform financial transactions to the total number of clients; *K7* – share of cash receipts from the total amount of receipts; *K8* – share of non-cash receipts from the total amount of receipts; K9 – share of cash expenditures from the total amount of expenditures. In addition, the availability of complete information about the considered set of banks is important for assessing the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on survival analysis methods. Thus, in the column *Censored* two possible values are defined: *completed* if complete information is available and *Censored* if there is no data about the occurrence of the event of interest.

Table 1. Input data base of the study

Bank name	Month_1	Day_1	Year_1	Month_2	Day_2	Year_2	*K1*	*K2*	...	*K8*	*K9*	Censored
A	1	2	3	4	5	6	7	8	9	10	11	12
VAT BANK FINANSY TA KREDYT	9	17	15	12	17	15	0.11	0.08		0.28	0.99	completed
AT BROKBUSINESSBANK	2	28	14	6	10	14	0.74	0.10		0.24	0.52	censored
VAT VTB BANK	11	27	18	12	18	18	0.12	0.13		0.20	0.54	completed
VAT KB NADRA	2	5	15	6	4	15	0.45	0.03		0.37	0.31	completed
AKB FORUM	3	13	14	6	13	14	0.34	0.09		0.15	1.15	completed
AKB IMEXBANK	1	26	15	5	21	15	0.19	0.03		0.36	0.50	completed
TOV KB DELTA	3	2	15	10	2	15	0.00	0.00		0.26	1.56	completed
PAT KB KHRESHCHATYK	4	5	16	6	2	16	0.01	0.08		0.25	0.59	completed
VAT RODOVID BANK	2	25	16	12	19	17	0.06	0.01		0.33	1.49	censored
PAT FINANSOVA INIT-SIATYVA	6	23	15	5	21	19	0.04	0.19		0.21	0.84	completed
...	...	...	...	...	...	...	...	...	...	...	...	...
AB UKOOPSPILKA	1	22	15	4	22	15	0.54	0.06		0.05	0.55	completed
TOV FORTUNA-BANK	1	26	17	2	21	17	0.03	0.60		0.35	1.16	completed
AKB TK KREDYT	2	9	16	4	7	16	0.22	0.69		0.73	1.56	completed
AKB INTEGRAL-BANK	9	15	15	11	25	15	0.64	0.50		0.56	1.68	censored
AKB NATSIONALNYY KREDYT	6	5	15	8	28	15	0.17	0.03		0.17	0.93	completed
VAT AB UKRGAZPROM-BANK	4	7	15	9	14	15	0.30	0.14		0.48	0.42	completed
VAT BANK TRAST	12	6	16	12	29	16	0.00	0.51		0.03	0.18	completed
PAT PtB	1	10	17	2	23	17	0.02	2.03		0.62	1.23	completed
VAT AKTABANK	9	16	14	1	15	15	0.04	1.35		0.37	1.92	completed
VAT ZLATOBANK	2	13	15	5	12	15	0.00	1.91		0.50	0.79	completed

Source: compiled by the authors

Stage 2 – ***Study of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on survival tables***. The technique of constructing survival tables is one of the methods for analysing survival data, which is based on a table of frequencies of possible occurrence of critical events in accordance with a certain selected number of intervals. In the context of the effectiveness of the national system for countering cyber fraud and money laundering, the approach based on survival tables allows building tables of the frequency of possible decision of the NBU to declare a bank insolvent or the NBU's decision to dissolve the bank as a result of monitoring activities and compliance with legislative standards. The Statistica software package was used to implement this stage. For this purpose, the following command was executed: Statistics / Linear / Nonlinear Models / Survival Analysis / Life labels and Distributions, that is, by selecting the command of the lifetime and distribution tables.

Stage 3 – ***Study of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on the Kaplan-Meyer method***. The advantage of using the Kaplan-Meier method in comparison with the life tables method described in the second stage is the fact that in this approach, performance estimates do not depend on grouping the observation interval into intervals. The Kaplan-Meier method involves evaluating survival function as follows:

$$KM(t) = \prod_{i=1}^{t} \left[\frac{n-i}{n-i+1}\right]^{\beta i} \quad (1)$$

where $KM(t)$ – survival function score; n – total number of observation objects (banks) of the studied sample; $\prod_{(i=1)}^{t}$ – the product (geometric sum) in the context of all observation objects (banks), the study of which was completed by the time t; βi – takes a single value if the observation in the context of the bank under study is not censored (completed), and a zero value if the observation in the context of the bank under study is censored (not completed, connection is lost); i – the observation number is not in the context of the bank under study in the source file, but the observation number in the new file, ordered by the number of days of "life" of banks.

The Statistica software package was used to implement this stage. The following command was executed: Statistics / Linear / Nonlinear Models / Survival Analysis / Kaplan and Meier product-limit method, that is, by selecting the Kaplan and Meyer product-limit method command.

Results and Discussion

Considering the results of the bibliometric analysis of papers for 2010-2020, a map of the relationship between the concept of "cyber fraud efficiency" and other scientific categories was formed. VOSviewer was the tool for implementing this map. This allowed selecting 7 clusters, which in Figure 1 are displayed as red, blue, green, blue, purple, yellow, and orange. It is worth noting that the larger size of the rectangle corresponds to a higher frequency of mentioning the category that is indicated in it as a key concept in relation to the category "cyber fraud efficiency".

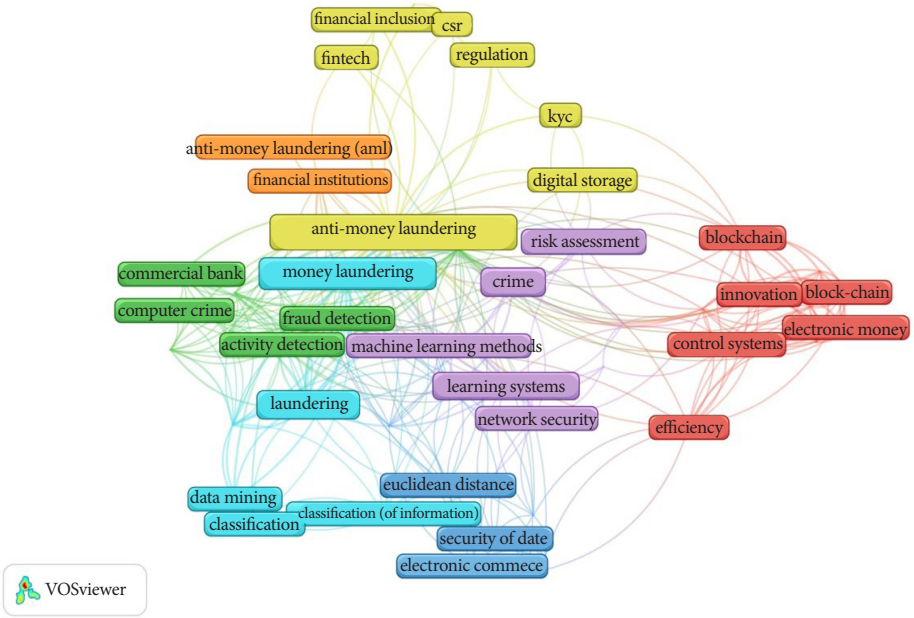

Figure 1. Scientific bibliography of the concept of "cyber fraud efficiency" using the VOSviewer 1.6.15 for the period from 2010 to 2020

Source: compiled by the authors

Analysing the results of the content and contextual block of bibliometric analysis, it is noted that the main array of research is focused on identifying the relationships between the efficiency of cyber fraud and countering money laundering obtained by criminal means (yellow cluster), crime and risk assessment (purple cluster), funds obtained by criminal means (blue cluster), blockchain and management system (red cluster), computer crime (green cluster), financial institutions (orange cluster), and data security (blue cluster). Thus, the fundamental categories in the study of the efficiency of cyber fraud are such categories as "countering money laundering", "funds obtained by criminal means", "crime" and the like. This is also proved by the data presented in Figure 2. Next, the study will analyse the contextual and temporal block of bibliometric analysis (Figure 2). The colour saturation in Figure 2 varies from dark purple (early publications) to yellow (modern publications).

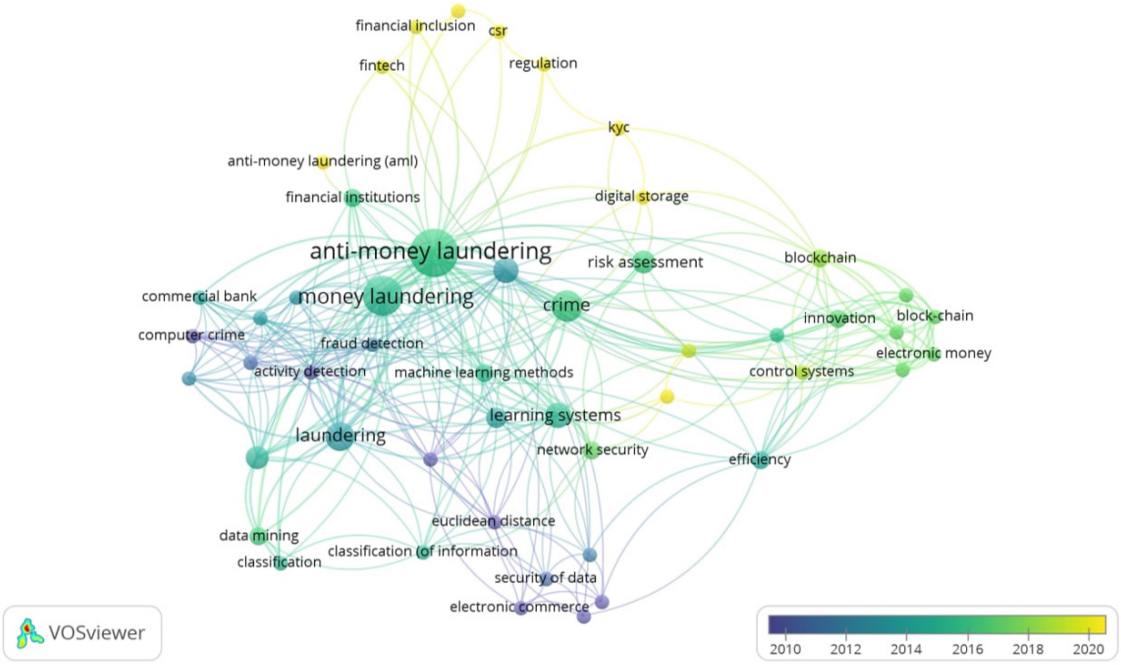

Figure 2. Visualisation map of the contextual and temporal dimension of research on the effectiveness of cyber fraud for 2010-2020 in publications of the Scopus database

Source: compiled by the authors

Thus, based on the results of contextual and temporal analysis on cyber fraud efficiency, three stages of changing research vectors were established, in particular: in 2010-2013, researchers tried to clearly understand and define how to interpret the concept of "cyber fraud", its types. During 2014-2018, researchers were concerned with countering cyber fraud, assessing the risks of its occurrence and establishing control over financial institutions as part of countering the legalisation of funds obtained by criminal means. In 2019-2020, with the development of electronic funds and blockchain, the main focus began to be on financial technologies and countering cyber fraud in modern realities.

At each of the conducted stages of implementation of economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation, the corresponding results of the study were formed. At the stage of studying the effectiveness of the national system for countering cyber fraud, a table of NBU decision-making frequencies on declaring banks insolvent or dissolution of banks is constructed based on survival tables (Table 1).

Table 1. NBU decision-making frequencies on declaring banks insolvent or their dissolution

	Life Table (Spreadsheet1.sta) Log-Likelihood for data: -43,6918																
Interval	Interval Start	Mid Point	Interval Width	Number Entering	Number Withdrwn	Number Exposed	Number Dying	Proportn Dead	Proportn Survivng	Cum. Prop Survivng	Problty Density	Hazard Rate	Std.Err. Cum. Surv	Std.Err. Prob. Den	Std.Err. Haz.Rate	Median Life Exp	Std.Err. Life Exp
Intno.1	0,00	64,91	129,82	70	23	58,5	42	0,718	0,282	1,000	0,006	0,009	0,000	0,000	0,001	90,409	11,820
Intno.2	129,82	194,73	129,82	5	1	4,5	2	0,444	0,556	0,282	0,001	0,004	0,059	0,001	0,003	181,745	220,309
Intno.3	259,64	324,55	129,82	2	0	2,0	0	0,250	0,750	0,157	0,000	0,002	0,074	0,000	0,003	317,333	326,383
Intno.4	389,45	454,36	129,82	2	0	2,0	0	0,250	0,750	0,118	0,000	0,002	0,073	0,000	0,003	302,909	244,787
Intno.5	519,27	584,18	129,82	2	0	2,0	0	0,250	0,750	0,088	0,000	0,002	0,066	0,000	0,003	259,636	183,591
Intno.6	649,09	714,00	129,82	2	1	1,5	0	0,333	0,667	0,066	0,000	0,003	0,056	0,000	0,004	194,727	158,994
Intno.7	778,91	843,82	129,82	1	0	1,0	0	0,500	0,500	0,044	0,000	0,005	0,045	0,000	0,007	129,818	259,636
Intno.8	908,73	973,64	129,82	1	0	1,0	0	0,500	0,500	0,022	0,000	0,005	0,032	0,000	0,007	129,818	259,636
Intno.9	1038,55	103,45	129,82	1	0	1,0	0	0,500	0,500	0,011	0,000	0,005	0,019	0,000	0,007	129,818	259,636
Intno.10	1168,36	233,27	129,82	1	0	1,0	0	0,500	0,500	0,006	0,000	0,005	0,011	0,000	0,007	129,818	259,636
Intno.11	1298,18	363,09	129,82	1	0	1,0	0	0,500	0,500	0,003	0,000	0,005	0,006	0,000	0,007	64,909	129,818
Intno.12	1428,00			1	0	1,0	1	0,500	0,500	0,001			0,003				

Source: compiled by the authors

Based on the data in Table 1, it can be concluded that for the selected set of Ukrainian banks, their activities are constantly monitored in the context of countering cyber fraud and criminal proceeds legalisation, and on average, in cases of violations within 1,428 days (i.e., 3.9 years), the relevant banks are given the opportunity to liquidate them or an appropriate management decision is made to declare banks insolvent, which acts as a quantitative characteristic of the effectiveness of the national system. Thus, during the first 129 days after the discovery of the facts of using banks to conduct cyber fraud among 70 banks considered in the sample (column *Number Entering*) the number of banks that were subject to verification and were not dissolved is 58 (column *Number Exposed*). During this time interval, the share of banks that have stepped up their activities in the context of countering cyber fraud is 28.2% (column *Proportion Surviving*), while the share of dissolved banks within 129 days after the NBU's decision to declare the bank insolvent is 71.8%. Moving to a different time interval – the next 129 days after the discovery of the facts of cyber fraud, the share of liquidated banks decreases to 44.4%, and the share of banks that have taken measures to counteract the existing offenses increases to 55.6 %. It is the indicator of the survival rate (graph Proportion Surviving) indicates the effectiveness of the national system for countering cyber fraud, which is constantly growing during the first three-time intervals (387 days) after the discovery of violations or the decision on the insolvency of banks from 0,282 shares of a unit to 0,750 shares of a unit. 3rd, 4th, and 5th time intervals of 129 days (i.e., from 387 to 645 days) remain constant at 0.750 fractions of a unit, which indicates a high level of efficiency. Further, starting from the 6th interval (774 days or 2.1 years) after identifying the facts of offenses or making a decision on the insolvency of banks, this efficiency begins to fall to 0.500 units.

The next interesting indicator from the standpoint of analysis is such an indicator as the probability density (graph Probability Density), that is, an assessment of the probability of making a decision to liquidate the bank in the appropriate time interval:

$$p_{li} = \frac{K_i - K_{i+1}}{w_i} \quad (2)$$

where p_{li} – estimation of the probability density of bank liquidation in the context of the *i*-th interval; K_i, $K_{(i+1)}$ – cumulative shares (survival functions) of banks that were not liquidated before the start of the *i*-th and *i+1*-th intervals; w_i – width of the *i*-th interval.

Based on the data obtained in Table 1 in terms of probability density, it can be concluded that the probability of dissolution of banks declared insolvent within the first 129 days is the highest and amounts to 0,006 parts of one. Over the next 129 days, this indicator decreases to 0,001 fractions of a unit.

An important factor in the context of this stage is the analysis of the indicator of the failure rate function or the instantaneous risk function (graph *Hazard rate* Table 1), which is defined as an estimate of the probability that a bank that survived (was not liquidated) before the start of the corresponding time interval will be liquidated within a given interval (the next 129 days for a given case). Analysis of this indicator shows the value of the instantaneous risk function at the level of 0,009 shares of one for the first time interval, that is, among 58 banks that were not liquidated after the decision on their insolvency was made, the instantaneous risk of making a decision on their liquidation is 0,009 shares of one. This risk gradually decreases to 0,002 fractions of a unit over 3rd, 4th, and 5th intervals (i.e., from 387 to 645 days), and then increases to 0,005 fractions of a unit at the end of the studied time period.

The results of the stage of research on the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on the Kaplan-Meyer method are presented in the form of an analysis fragment (Table 2).

Table 2. Results of the analysis of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on the Kaplan-Meyer method (fragment)

	Kaplan-Meier (Product-limit) analysis (Spreadsheet1.sta Note: Censored cases are marked with +		
Case Number	Time	Cumulatv Survival	Standard Error
32+	20,000		
3	21,000	0,985507	0,014387
67	23,000	0,971015	0,020197
44+	24,000		
62	26,000	0,956302	0,024674
34+	27,000		
56+	30,000		
58+	30,000		
47	35,000	0,940878	0,028695
36+	43,000		
68	44,000	0,925197	0,032218
55+	44,000		
60+	47,000		

Source: compiled by the authors

Analysing the effectiveness of the national system for countering cyber fraud based on the Kaplan-Meier method based on the data in Table 2, censored banks (with incomplete data) are marked with a + sign. In Table 2, all the banks studied are grouped by the number of days (graph *Time*), during which the bank performed its activities in the context of countering cyber fraud and criminal proceeds legalisation after the revealed facts of violations and the NBU's decision on insolvency. Graph *Cumulative Survival* in Table 2 indicates the probability that the relevant bank will "survive" (will not be liquidated for violations in the context of cyber fraud and legalisation of criminal proceeds) and implement counteraction measures. Consequently, the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation is the highest at the level of at least 95% in the first 26 days after the detection of offenses. This indicator decreases to 90% in the interval of up to 55 days (approximately two months); to 80% in the interval of up to 75 days (two and a half months), to 50% in the interval of up to 93 days (three months), that is, the effectiveness of measures to counter cyber fraud will rapidly decrease with increasing time that has passed since the discovery of offenses. Figure 3 graphically presents the detected dependency.

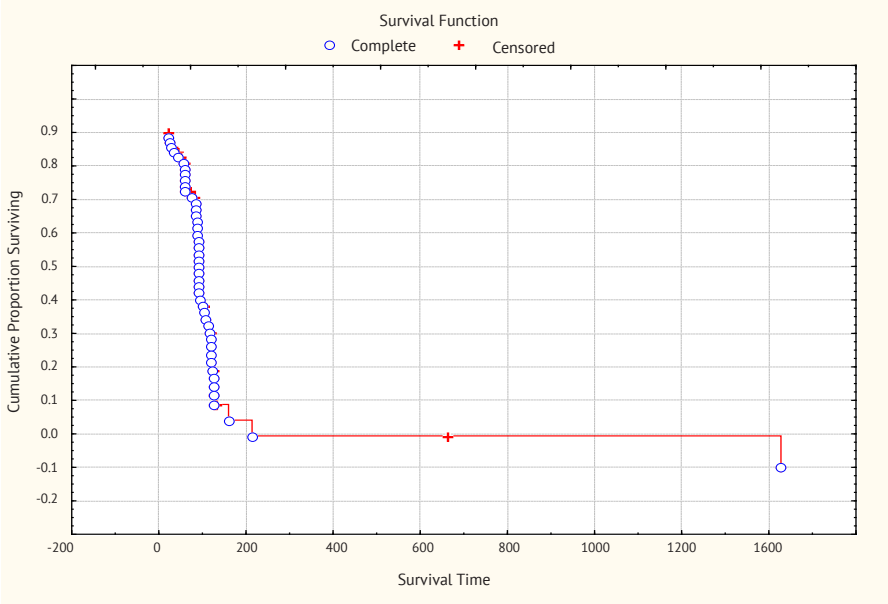

Figure 3. Visualisation of the dependence of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation (based on the Kaplan-Meier method) on the time interval after the detection of violations

Source: compiled by the authors

The graph in Figure 3 shows that the value of the survival function drops sharply in the first 93 days after the detection of violations. For ease of interpretation of the results, complete observations are marked with dots, and incomplete observations are marked with crosses.

In order to reflect the nature of the distribution of the effectiveness of the national system of countering cyber fraud, presented in Figure 3, Table 3 is constructed. It presents the percentage ratio: 25% (lower quartile) – banks for which the decision on dissolution is made, that is, appropriate measures are taken in the context of countering offenses, within the first 85 days after the discovery of these facts, 50% (median) – reflect banks that activate counteraction measures for no more than 93 days (3 months). The decision on the largest number of banks (75%) and measures to counter cyber fraud is made within 124 days after the facts of offenses are revealed, that is, within 4 months.

Table 3. Percentile survival functions of distribution of banks for which a decision on dissolution is made

	Percentiles of (Spreadsheet1 the Survival Function
Percentiles	Survival Time
25'th percentile (lower quartile)	85,0255
50'th percentile (median)	93,8276
75'th percentile (upper quartile)	124,0000

Source: compiled by the authors

The current national system for countering cyber fraud and criminal proceeds legalisation still has certain gaps that hinder its effectiveness. And to achieve such comprehensive efficiency, certain economic and mathematical models are used, aimed at effectively countering the laundering of illegal income, combating cybercrime and cyber fraudsters. It should be noted that economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation clearly demonstrates the scientific significance and practical importance of applying complex models in the study of financial and economic processes and actions, which in its result allows us to get positive results in stabilising the country's economic security.

Taking into account the above, the authors emphasise that the proposed modelling based on methods of survival analysis would allow financial analysts both at the state level and at the level of business entities to analyse, understand, evaluate, and predict financial and economic processes and the likely consequences of their occurrence in time in the line of countering cybercrime and preventing the legalisation of illegal income. This will allow foreseeing possible scenarios for the occurrence of negative consequences from possible fraudulent attacks on the state's economic system, developing and implementing measures to combat financial and economic crimes in a timely and effective manner.

Conclusions

Thus, in the conducted study, a bibliometric analysis of existing papers concerning the problems of the effectiveness of cyber fraud and countering the legalisation of funds obtained by criminal means is carried out. As a result, based on the VOSviewer software, a bibliometric map of keywords and concepts of research papers is built. The conducted research allowed more thoroughly formalising the theoretical aspects of the spread of cyber fraud and criminal proceeds legalisation in modern conditions within the framework of contextual, evolutionary, and spatial analysis. Among the fundamental categories of analysis of the effectiveness of cyber fraud, such concepts as "anti-money laundering", "funds obtained by criminal means", "crime" and others were identified. It is also established that insufficient attention is paid to cyber fraud and money laundering in the economic sectors, although in recent years, due to the development of digitalisation and e-commerce, the problem has become more urgent and causes significant damage to the economy.

The article implements economic and mathematical modelling of the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation, which is based on the use of survival analysis methods. For this purpose, at the first stage, the input data base was formed from 9 selected indicators for 70 banks of Ukraine for 2019. At the second stage, the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on survival tables was investigated. The third stage investigated the effectiveness of the national system for countering cyber fraud and criminal proceeds legalisation based on the Kaplan-Meyer method, including assessing the survival function and risk function. And as a result of the conducted modelling, the dependence of the effectiveness of the national system for countering cyber fraud and legalisation of criminal proceeds obtained illegally on the time interval after the detection of violations was revealed.

Acknowledgements

The study was performed within the framework of the research topic "Data-Mining to counteract cyber fraud and criminal proceeds legalisation in the context of digitalisation of the financial sector of the economy of Ukraine" (State Registration number 0121U100467) and state budget research work No. 0121u109559 "National security through the convergence of financial monitoring and cybersecurity systems: intelligent modelling of financial market regulation mechanisms".

References

[1] De Koker, L., & Tran, T.T.H. (2021). Confiscation of proceeds of crime in Vietnam: Improving the legal framework. *Journal of Money Laundering Control*. doi:10.1108/JMLC-11-2020-0123.

[2] Lebid, O., & Veits, O. (2020). Search for statistically approved criteria for identifying money laundering risk. *Banks and Bank Systems*, 15(4), 150-163. doi: 10.21511/bbs.15(4).2020.13.

[3] Levi, M. (2020). Evaluating the control of money laundering and its underlying offences: The search for meaningful data. *Asian Journal of Criminology*, 15(4), 301-320. doi: 10.1007/s11417-020-09319-y.

[4] Vovk, V., Zhezherun, Y., Bilovodska, O., Babenko, V., & Biriukova, A. (2020). Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalization of economy: Management and legal aspects of the risk-based approach. *International Journal of Industrial Engineering and Production Research*, 31(4), 559-570. doi: 10.22068/ijiepr.31.4.559.

[5] Chen, S., Yuan, Y., (Robert) Luo, X., Jian, J., & Wang, Y. (2021). Discovering group-based transnational cyber fraud actives: A polymethodological view. *Computers and Security*, 104, article number 102217. doi: 10.1016/j.cose.2021.102217.

[6] Kara, I., & Aydos, M. (2020). Cyber fraud: Detection and analysis of the crypto-ransomware. In *11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, (UEMCON)* (pp. 0764-0769). New York: IEEE. doi:10.1109/UEMCON51285.2020.9298128.

[7] Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research,* 26(3), 293-312. doi: 10.1007/s10610-020-09439-2.

[8] Lux, L.M., & Calderón, G.O. (2020). The crime of cyber fraud: Definition and delimitation. *Revista Chilena De Derecho y Tecnologia,* 9(1), 151-184. doi: 10.5354/0719-2584.2020.57149.

[9] Ferwerda, J., van Saase, A., Unger, B., & Getzner, M. (2020). Estimating money laundering flows with a gravity model-based simulation. *Scientific Reports,* 10(1), article number 18552. doi: 10.1038/s41598-020-75653-x.

[10] Safronova, T.I., Vladimirov, S.A., & Prikhodko, I.A. (2021). Probabilistic approach to soil fertility conservation by mathematical modeling of technological processes and optimization of resource use. *IOP Conference Series: Earth and Environmental Science*, 666, article number 042063. doi: 10.1088/1755-1315/666/4/042063.

[11] Borodin, A., Mityushina, I., Streltsova, E., Kulikov, A., Yakovenko, I., & Namitulina, A. (2021). Mathematical modeling for financial analysis of an enterprise: Motivating of not open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(1), 1-16. doi: 10.3390/joitmc7010079.

[12] Wubneh, K.G., Desta, F.M., & Kahsay, H.A. (2021). Mathematical modeling and analysis of khat-chewing dynamics. *Journal of Mathematics*, 2021, article number 665955. doi: 10.1155/2021/6659551.

[13] Shoaee, S., & Khorram, E. (2020). Survival analysis for a new compounded bivariate failure time distribution in shock and competing risk models via an EM algorithm. *Communications in Statistics – Theory and Methods*, 49(21), 5123-5153.

[14] Platero, C., & Tobar, M.C. (2020). Longitudinal survival analysis and two-group comparison for predicting the progression of mild cognitive impairment to Alzheimer's disease. *Journal of Neuroscience Methods*, 341, article number 108698. doi: 10.1016/j.jneumeth.2020.108698.

[15] Stevens, N., Lydon, M., Marshall, A.H., & Taylor, S. (2020). Identification of bridge key performance indicators using survival analysis for future network-wide structural health monitoring. *Sensors (Switzerland),* 20(23), 1-15.