

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY
Academic and Research Institute of Business, Economics and Management
Department of Economic Cybernetics

«Admitted to the defense»

Head of Department

_____ Koibichuk V. V.

(signature)

(First and LAST NAME)

_____ 20__ p.

QUALIFICATION WORK

to obtain an educational degree bachelor_____

(bachelor / master)

from the specialty 051 Economics _____,

(code and name)

educational-professional _____ programs Business Analytics_____

(educational-professional / educational-scientific)

(the name of the program)

on the topic: Economic and mathematical modeling of due diligence of enterprises in the combating financial cyber frauds aspect based on data mining methods

Winner(s) of the group AB-91a.an ___ Daryna Evgenivna Berezhna _____

(group cipher)

(full name)

The qualification work contains the results of own research. The use of ideas, results and texts of other authors are linked to the corresponding source



(signature)

Berezhna D. E.

(Name and SURNAME of the acquirer)

Head Doctor of Philosophy, Assistant Dotsenko T. _____

(position, academic degree, academic title, Name and SURNAME)



(signature)

Consultant _____

(position, academic degree, academic title, Name and SURNAME)

(signature)

Sumy – 2023

SUMMARY

bachelor's qualification work on the topic

"ECONOMIC AND MATHEMATICAL MODELING OF DUE DILIGENCE OF ENTERPRISES IN THE COMBATING FINANCIAL CYBER FRAUDS ASPECT BASED ON DATA MINING METHODS"

Student Daryna Evgenivna Berezhna

(Full Name)

Relevance of the research topic. Fraud is a significant risk for the financial and economic security and stability of modern business entities. They may occur due to the lack of clear clarity of the organization's functioning, improper activity of the institution, deficiencies in information and technical support, financial issues. Also, technical skills and advances in technology are becoming more accessible to criminals. Therefore, it is becoming more difficult to deal with the tactics of committing modern criminal crimes using traditional methods. In order to prevent fraud, in order to ensure the safe and uninterrupted functioning of enterprises, increase the efficiency of economic activity, and preserve assets, it is necessary to introduce a system of reliable protection of subjects based on the use of various mechanisms and tools. In order to prevent fraud, based on the specifics of the functioning of enterprises, it is necessary to conduct their inspection. Such checks are audit, assessment, tax audits, due diligence procedure.

First of all, the reliability of the enterprise is determined by its financial security. And in the conditions of digitalization of the economy, which is growing at a rapid pace, and which has been decisive in the activities of enterprises in recent years, a system of financial cyber protection appears. And to combat financial cyber fraud, as one of the newest methods, the use of the Due Diligence tool is proposed. This will help increase the financial cyber protection of the enterprise, which will facilitate the achievement of strategic goals, increase the value of business, and expand competitive advantages.

Thus, in the modern digitalized conditions of the functioning of business entities, the improvement of the financial protection system, including through the use of such a verification procedure as Due Diligence, which is particularly effective in the aspect of countering financial cyber fraud, becomes particularly relevant.

The purpose of the work – studying and deepening the theoretical aspects of due diligence of enterprises in the aspect of countering financial cyber fraud, identifying the main factors and developing a structural and logical model of due diligence of enterprises in the aspect of countering financial cyber fraud .

The tasks of the work are: to characterize the subject field and identify the most important parameters of the research object; to analyze the current state of modeling of the research object; to form a statement of the modeling task and requirements for the model; develop a mathematical model; check the adequacy of the constructed mathematical model; to build a method of design calculations; to develop a software application for automating calculation methods.

The object of the study is the due diligence of enterprises in the aspect of combating financial cyber fraud.

The subject of the research is mathematical methods and data mining models for assessing due diligence of enterprises in the aspect of countering financial cyber fraud.

Research methods: theoretical analysis of literature (to study theoretical concepts, directions and aspects of the researched topic); bibliometric analysis (analysis of scientific publications of the Scopus database by key research categories, using the VOSViewerv.1.6.15 toolkit); Bizagi Modeler software (for building a structural and logical diagram of the stages and features of due diligence implementation of enterprises); applied statistical package Statistica 10 and Statistica Portable (for building a model); cluster analysis, k-means method, dispersion analysis (for grouping countries into clusters); factor analysis, methods of sigma-limited parameterization and correlation analysis (to represent relevant factors); regression analysis, construction of multiple linear regressions using the method of least squares

- OLS-method (to establish the dependence between factors, to determine the strength of influence and the direction of influence of factors).

Information base. The qualification work is performed on the statistical data of The World Bank, Global Digital Convergence, Digital Development Dashboard, NCSI for 2021, the resource base of the Scopus information platform, training manuals, scientific publications of foreign and domestic researchers.

The main scientific result of the qualification work. The scientific result of the qualification work consists in the development of a structural-logical economic-mathematical model of due diligence of enterprises in the aspect of combating financial cyber-frauds, which was formed on the basis of a set of special research methods, cluster analysis, k-means method; factor analysis, methods of sigma-limited parameterization and correlation analysis; regression analysis, construction of multiple linear regressions using the method of least squares - OLS-method.

Recommendations on the use of research results. The practical significance of the obtained results is that the results of the conducted scientific research can be used at enterprises to form guiding principles and policies of financial security of enterprises, which in turn will help to reduce the level of negative consequences, including financial cyber threats, financial cyber risks that may be present in business processes; to maximize possible positive effects from the adoption of management decisions formed taking into account a number of factors.

Approbation of research results. Tetiana Dotsenko, Hanna Yarovenko, Darina Berezhna. Due diligence in the aspect of countering financial cyber fraud: modeling trends. Economic Bulletin of the State Higher Educational Institution "Ukrainian State Chemical and Technological University". Submitted for publication on 19.05.2023.

Keywords: due diligence, combating financial cyber fraud, level of cyber security, data mining, cluster analysis, k-means method, factor analysis, correlation analysis, regression analysis.

The content of the qualification work is laid out on 69 pages. List of used

sources with 38 names, placed on 6 pages. The work contains 2 tables, 46 figures, as well as 3 appendices, located on 16 pages.

The year of completion of the qualification work is 2023.

The year of job protection is 2023.

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SUMY STATE UNIVERSITY
Academic and Research Institute of Business, Economics and Management
Department of Economic Cybernetics

APPROVE

Head of Department

V. Koibichuk

“03” April 2023

TASKS FOR BACHELOR'S QUALIFICATION WORK

Specialty 051 Economics (BusinessAnalytics)

Fourth Year Student, Group.AB - 91a. an

Darina Berezhna

1. Topic of work «Economic and mathematical modeling of due diligence of enterprises in the combating financial cyber frauds aspect based on data mining methods» approved by the order On approval of topics and supervisors of qualification works наказ №0553-VI from 23.05.2023 year.
 2. Deadline for submission of finished work by the student «03» June 2023 year
 3. The purpose of the qualification work: development of a structural and logical model of due diligence of enterprises in the aspect of combating financial cyber fraud.
 4. Object of research: due diligence of enterprises in the aspect of countering financial cyber fraud.
 5. The subject of the research: mathematical methods and data mining models for assessing the due diligence of enterprises in the aspect of combating financial cyber fraud.
 6. Qualification work is performed on the basis of legislative and regulatory acts, statistical data of the National Bank of Ukraine and the European Central Bank, training manuals, scientific publications of foreign and domestic researchers
 7. Tentative plan of qualification work, deadlines for submission of sections to the manager and content of tasks to fulfill the set goal
- Chapter 1. General characteristics of the research object and construction of a mathematical model
- (name – submission deadline)

In section 1.

1.1 Analysis of the subject area and identification of the most significant parameters of the research object.

1.2 Overview of the current state of research object modeling.

1.3 Setting the modeling task and forming requirements for the model.

1.4 Development of a mathematical model.

Section 2. Verification of model adequacy and proposals for its use

(name – submission deadline)

In section 2.

2.1 Checking the adequacy of the constructed mathematical model.

2.2 Construction of the methodology of design calculations.


2.3 Development of a software application for automating calculation methods.

8. Консультації з роботи:

Section	Surname, initials and position of the consultant	Signature, date	
		issued the task	accepted the task
1	Tetiana Dotsenko	03/04/2023	03/04/2023
2	Tetiana Dotsenko	04/06/2023	04/06/2023

9. Issue date of the assignment: «03» April 2023 year


Head of qualification work



(підпис)

T. Dotsenko
(ініціали, прізвище)

Tasks to be completed received



(підпис)

D. Berezhna
(ініціали, прізвище)

CONTENT

INTRODUCTION	9
CHAPTER 1. GENERAL CHARACTERISTICS OF THE RESEARCH OBJECT AND MATHEMATICAL MODEL CONSTRUCTION	12
1.1. Analysis of the subject area and identification of the most significant parameters of the research object.....	12
1.2. Overview of the current state of research object modeling	18
1.3. Statement of the modeling problem and formulation of model requirements	29
1.4. Mathematical model development	30
CHAPTER 2. VERIFICATION OF THE ADEQUACY OF THE MODEL AND PROPOSALS FOR ITS USE	39
2.1. Checking the adequacy of the constructed mathematical model	39
2.2. Construction of the methodology of design calculations.....	44
2.3. Development of a software application for automating calculation methods.....	57
CONCLUSIONS	67
REFERENCES	69
APPENDIXES.....	76

INTRODUCTION

Fraud is a significant risk for the financial and economic security and stability of modern business entities. They may occur due to the lack of clear clarity of the organization's functioning, improper activity of the institution, deficiencies in information and technical support, financial issues. Also, technical skills and advances in technology are becoming more accessible to criminals. Therefore, it is becoming more difficult to deal with the tactics of committing modern criminal crimes using traditional methods. In order to prevent fraud, in order to ensure the safe and uninterrupted functioning of enterprises, increase the efficiency of economic activity, and preserve assets, it is necessary to introduce a system of reliable protection of subjects based on the use of various mechanisms and tools. In order to prevent fraud, based on the specifics of the functioning of enterprises, it is necessary to conduct their inspection. Such checks are audit, assessment, tax audits, due diligence procedure.

First of all, the reliability of the enterprise is determined by its financial security. And in the conditions of digitalization of the economy, which is growing at a rapid pace, and which has been decisive in the activities of enterprises in recent years, a system of financial cyber protection appears. And to combat financial cyber fraud, as one of the newest methods, the use of the Due Diligence tool is proposed. This will help increase the financial cyber protection of the enterprise, which will facilitate the achievement of strategic goals, increase the value of business, and expand competitive advantages.

Thus, in the modern digitalized conditions of the functioning of business entities, the improvement of the financial protection system, including through the use of such a verification procedure as Due Diligence, which is particularly effective in the aspect of countering financial cyber fraud, becomes particularly relevant.

The main task of ensuring information security is increasingly being solved as a result of improving the information management process based on the implementation of various approaches and methods, compliance with regulatory requirements and the application of organizational measures. In the conditions of Ukraine as an independent state, the role of economic-mathematical methods is growing as one of the ways to develop a dynamically developed and stable economy with scientifically based development paths and forecasts for the future at the transition stage to the market.

Therefore, in order to ensure the appropriate level of information security, it is necessary to build an information risk management system, monitor and support it, which will allow the effective use of a combination of all possible means and methods. For this, it is necessary to comply with the requirements specified in the standards for ensuring information security and risk assessment.

The purpose of the work – studying and deepening the theoretical aspects of due diligence of enterprises in the aspect of countering financial cyber fraud, identifying the main factors and developing a structural and logical model of due diligence of enterprises in the aspect of countering financial cyber fraud.

The tasks of the work are: to characterize the subject field and identify the most important parameters of the research object; to analyze the current state of modeling of the research object; to form a statement of the modeling task and requirements for the model; develop a mathematical model; перевірити адекватність побудованої математичної моделі; побудувати методику проектувальних розрахунків; розробити програмний застосунок для автоматизації методики розрахунків.

The object of the study is the due diligence of enterprises in the aspect of combating financial cyber fraud.

The subject of the research is mathematical methods and data mining models for assessing due diligence of enterprises in the aspect of countering financial cyber fraud.

Research methods: theoretical analysis of literature (to study theoretical

concepts, directions and aspects of the researched topic); bibliometric analysis (analysis of scientific publications of the Scopus database by key research categories, using the VOSViewerv.1.6.15 toolkit); Bizagi Modeler software (for building a structural and logical diagram of the stages and features of due diligence implementation of enterprises); applied statistical package Statistica 10 and Statistica Portable (for building a model); cluster analysis, k-means method, dispersion analysis (for grouping countries into clusters); factor analysis, methods of sigma-limited parameterization and correlation analysis (to represent relevant factors); regression analysis, construction of multiple linear regressions using the method of least squares - OLS-method (to establish the dependence between factors, to determine the strength of influence and the direction of influence of factors).

Information base. The qualification work is performed on the statistical data of The World Bank, Global Digital Convergence, Digital Development Dashboard, NCSI for 2021, the resource base of the Scopus information platform, training manuals, scientific publications of foreign and domestic researchers.

CHAPTER 1. GENERAL CHARACTERISTICS OF THE RESEARCH OBJECT AND MATHEMATICAL MODEL CONSTRUCTION

1.1. Analysis of the subject area and identification of the most significant parameters of the research object

The concept of due diligence is a relatively new category that is being actively used among modern scientists of the world. Discussions surrounding the theoretical and practical study of this issue are given in the works of such scientists as: Elbel J., Bose O'Reilly S. [12] regarding the impact and consequences of the European Union Law on Due Diligence on the activities of small businesses; Deva S. [10], Villiers, C. [37], Liesa C. R.F. [22], Sedano T.G. [34] regarding discussions of legislative and legal issues Due diligence; Litwin D. [24] regarding due diligence of economic inequality, the impact of business on inequality; Guanipa H.J., Chimá J. T. [13], Camoletto S. [6] on corporate due diligence, including corporate responsibility; etc.

One of the main reasons for inspections is the risks and threats of fraud, illegal activities, especially financial crimes and, according to recent trends, cyber fraud. The problems of combating financial cyber fraud have been actively studied by scientists in recent years: they are conducting an evolutionary study of approaches to combating financial cybercrime Nicholls J., Kuppa A., [29]; study the features of combating fraud caused by technology Dadhich M., Hiran K. K. [9]; carry out an evaluation of the effectiveness of the system for countering the legalization of illegal money Lieonov S., Hlawiczka R., Boiko A., Mynenko S., Garai-Fodor M. [22]; predict information trends for countering cybercrime risks Kuzior A., Brožek P., Kuzmenko O., Yarovenko H., Vasilyeva T. [19]; on the investigation of cybercrimes Bello M., Griffiths M. [3]; etc.

Moreover, in the direction of combating financial fraud, including cyber fraud, practitioners are beginning to use elements of the due diligence method of enterprises: Kalina I., Khurdei V., Shevchuk V., Vlasiuk T., Leonidov I. [14] describe

the application of the due diligence procedure due diligence of objects to manage the risks of corporate economic security; Chitimira H., Munedzi S. [8] highlight customer due diligence measures used to identify and combat money laundering; etc.

We emphasize that a special role in the study of economic processes is assigned to modeling, as an effective means of studying, analyzing, evaluating, forecasting certain phenomena and processes. Currently, various modeling techniques are actively used, namely: numerical and mathematical modeling (systems of differential equations) – Khan M. R., Puneeth V., Alqahtani A. M., Alhazmi S. E., Beinane S. A. O.[15]; information modeling (information analysis) – Lu T., Wang C., Cao Y., Chen H.[28]; economic modeling – Botchway S., Tsiachristas A., Pollard J., Fazel S. [4]; structural modeling – Attiany M. S., Al-Kharabsheh S. A., Al-Makhariz L. S., Abed-Qader M. A., Al-Hawary S. I. S. [2]; and many others.

To study the development of world scientific opinion in the direction of studying the trends of financial crime, it is advisable to first conduct a bibliometric analysis of the data of scientific assets, which can be implemented on the Scopus database, by using the VOSViewerv.1.6.15 toolkit.

The initial stage of the bibliometric analysis of the published scientific treatises of the Scopus database for 2014–2021 was the formation of a map of the relationships between the key terms "due diligence" and other scientific concepts. Analysis of the resulting map shows that the system selected 60 concepts most closely related to the studied categories. These concepts are grouped into 4 clusters of interrelated scientific terms (Figure 1.1), which are visually represented by different colors: 15 concepts are depicted in birch color, 13 concepts in purple, 15 concepts in blue, 8 concepts in light green, 7 concepts in yellow. Note that the larger size of the circles means a higher number of mentions of the category in studies of such a scientific concept, which is located in it, as a key concept that is interconnected with the researched concepts of "due diligence cyber security".

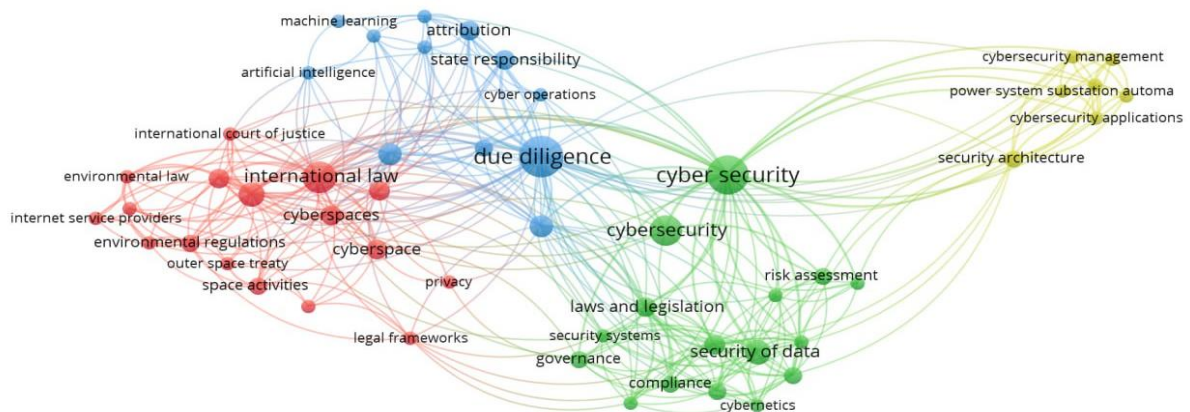


Figure 1.1 – Scientific bibliography of the concepts of "due diligence cyber security" for the period 2014–2021 using software tools

Thus, while conducting a content-contextual analysis of the received blocks of bibliometric analysis, we note that the largest sizes of circles, that is, the highest, fundamental influence in the study of "due diligence, cyber security" issues, are divided into 4 clusters: Cluster 1 (17 items) computers, international law, privacy, space activities, trans-boundary. Cluster 2 (16 items) cybernetics, compliance, governance, laws and legislation, security systems. Cluster 3 (12 items) artificial intelligence, crime, machine learning, malware, sovereignty. Cluster 4 (7 items) cybersecurity application, security architecture, security controls, substation automation.

Studying the evolutionary-time perspective of the research, a map of the relationships of the studied key concepts "due diligence cyber security" with other scientific categories for the period 2014–2021 in dynamics was built, and the contextual-time block of bibliometric analysis was analyzed. As a result, the grouping of important determinants of the analysis of financial crime trends in different time periods is clearly depicted (Figure 1.2), using different saturation of colors from purple to yellow, that is, from early publications to modern ones.

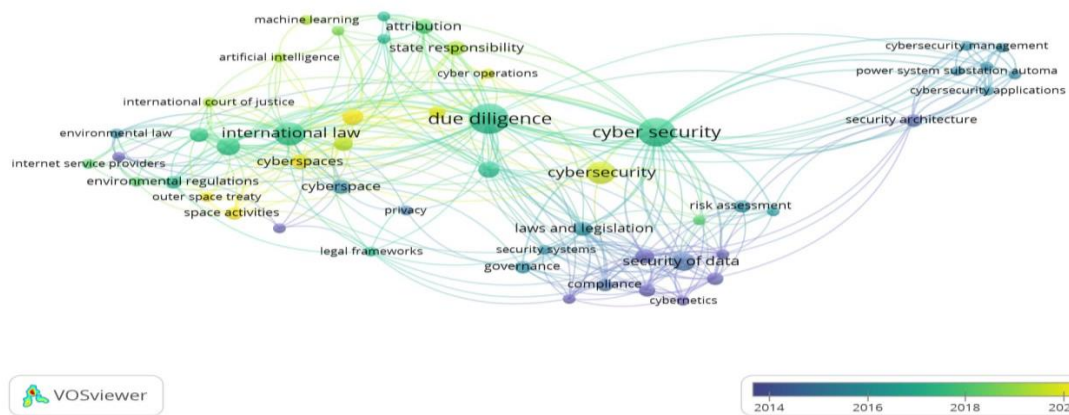


Figure 1.2 – Visualization map of the contextual-temporal dimension of scientific assets in the editions of the Scopus database of concepts "due diligence –cyber security" for the period 2014–2021 in dynamics, using the software tool VOSViewerv.1.6.15

Thus, according to the analysis of the contextual-temporal block of scientific publications of the Scopus database of the categories "due diligence - cyber security" for the period 2014–2021 in dynamics, three main stages in the directions of research are outlined. In particular, from 2014 to 2016 the theoretical, regulatory, and legislative foundations of the possibility of conducting cybercrimes on the Internet and their detection were studied. In the framework of 2017–2019, scientific interests were focused on the research of digital technologies, the storage of large-scale information, the use of extensive networks, numerous sites, the introduction of online services, the circulation of cryptocurrencies, which also contributed to the spread of cyber fraud and the growth of the capabilities of cyber criminals. In recent years 2019–2021, the vectors of modern researchers are increasingly directed towards machine learning, risk assessment, modeling, forecasting, and algorithmization of financial processes.

In turn, the bibliometric analysis of scientific publications dedicated to the study of the latest trends in financial crime made it possible to meaningfully systematize and formalize theoretical achievements in a certain direction, to implement a substantive-contextual, evolutionary-dynamic study of the key

categories of "financial crimes, cybercrime". It has been established that financial crime has been studied for a long time, but aspects of cybercrime are relatively new and will require in-depth consideration.

After analyzing the literature on the researched issue, the concept of Due Diligence (due diligence, examination) was formulated – as a scientific category, which involves carrying out a set of actions: multi-vector research and evaluation of the subject's work, with a deep study of the financial condition, risk assessment (including financial, investment), analysis of the object's place on the market, with a special emphasis on issues related to security, human rights and the environment – to form a comprehensive conclusion regarding the financial, legal, investment status of the subject of the study, existing risks. Due Diligence includes the following stages: searching and collecting data, studying, consolidating and analyzing data, forming a conclusion about the state of the enterprise on the investigated issue, making the appropriate decision.

In the economic sense, due diligence (hereinafter DD) means a deep and comprehensive analysis of all aspects of the company's activity: organizational, legal, financial, marketing, tax, political, market technological.

The need to conduct a DD arises in the following cases: in the process of making a decision on the admission of securities for quotation on the stock exchange; in the case of raising equity capital by enterprises whose corporate rights do not circulate on the market; in the process of reorganization of enterprises; in the process of rehabilitation of enterprises. DD is a necessary prerequisite for decision-making by large companies regarding the acquisition/absorption of other enterprises.

The normative basis of due diligence is the Proposal for the Directive of the European Parliament and the Council on due diligence of corporate sustainable development dated February 23, 2022. The legislative act of the European Union on Due Diligence is aimed at achieving the goals of sustainable development of the UN, in particular areas related to human rights and the environment, security, mitigation

of negative impacts on them. What will allow to form effective business solutions to protect organizations, ensure long-term sustainability of enterprises.

Due Diligence mainly includes a compliance check, during which operational activities, relations with counterparties and government bodies, possible adverse factors of the company's activity, etc. are comprehensively considered.

Depending on the needs of the Due Diligence procedure, the following types are distinguished (Table 1.1).

Table 1.1 – Types of Due Diligence

№	Назва	Опис
1	General Due Diligence	a comprehensive review of the main aspects of the company's activities, including financial status, taxation, legal aspects, management, the company's market share, etc.
2	Financial Due Diligence	verification of the financial condition of the company, in particular, assets and liabilities from the point of view of their assessment (the presence of off-balance sheet liabilities, depreciation of stocks, etc.)
3	Tax Due Diligence	identification of tax risks and objective assessment of all tax aspects of doing business.
4	Legal Due Diligence	analysis of legal aspects of the company's work, for example, registration of intellectual property rights, court cases, etc.
5	Vendor Due Diligence	the customer of which is the company itself or its current owner.
6	Operational Due Diligence	verification of operational activity, in particular, the level of loading of production facilities, the possibility of changing the assortment and increasing production.
7	Technological Due Diligence	study of production technology, state of equipment.

Due Diligence, among other things, allows you to determine and form an understanding of the state of financial protection of the subject under investigation, in particular, its financial cyber security, to ensure countermeasures against financial crimes and financial cyber fraud. To implement due diligence of enterprises in the aspect of combating financial cyber fraud, it is advisable to define a number of stages and features regarding its implementation. Figure A.1 shows the structural and logical diagram of the stages and features of due diligence implementation of enterprises built during the research. The scheme is built using Bizagi Modeler software.

1.2 overview of the current state of research object modeling

Among the methods of economic and mathematical modeling, models based on data mining methods are widely used, presented in the works of such scientists: Vasilyeva T., Ziółko A., Kuzmenko O., Kapinos A., Humenna Y. [36] – use methods of intellectual analysis data, such as AML scenarios based on the classification tree method (one-dimensional branching method CART), as well as clustering of countries according to relevant AML scenarios based on agglomeration methods to ensure effective management; Kuzmenko O., Šuleř P., Lyeonov S., Judrupa I., Boiko A. [18] – offer intelligent data analysis and bifurcation analysis to assess the risk of using financial institutions to launder criminal proceeds; Zarrabeitia-Bilbao E., Jaca-Madariaga M. [39] – apply a new approach to combining social network analysis methods with the use of artificial neural network models; Kumagai A., Jeong S., Kim D. (2023) [16] – describe the application of intelligent data analysis models to analyze the effectiveness and accuracy of medical tests; Ren D., Wang C., Wei X. [30] – propose multimodal data analysis for forecasting in materials science; etc.

When studying the concept of due diligence in depth, it is impossible not to note the importance of modeling its processes and stages. These issues are highlighted by the following experts: Carannante, M., D'Amato, V., Fersini, P., [7] propose a due diligence model based on machine learning; Roy V., Desjardins D., Fertel C., [31] developed a due diligence model based on risk assessment; Aman, A., & Reji, D. J. [1] reveal the features of building a due diligence model based on deep learning of NLP; Li Z. [27] describes the NAP, mHRDD, BHR models of the optimality of evaluating the implementation of the UN guidelines on business and human rights; Liu W., Sun Y. [25] interpret the model of consensus multidimensional verification of investment projects based on financial technologies; Liu Y., Feng Y., [26] propose a computer model of due diligence through AHP and big data.

In addition, we should focus on modeling in the aspect of combating financial cyber fraud, as a defining component of the researched issue. Namely: Lin K., and Gao Y. [23] propose a SHAP group method model for financial fraud detection; Vasilyeva T. A., Kuzmenko O. V., Stoyanets N. V., Artyukhov A. E., Bozhenko, V. V. [35] developed a complex model for creating a phase image of a cybercrime victim based on the methods of systematization, comparison, grouping, logical generalization, bibliometric analysis, regression analysis (the method of sigma-limited parameterization), algorithm of associative rules; Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brožek P. (2022) [20] present an econometric model of the impact of digitalization on economic transformations based on developed quantile regressions (taking into account the national cyber security indicator); Kuzmenko O. V., Kubálek J., Bozhenko V. V., Kushneryov O. S., Vida, I. [19] highlight Machine Linked Learning (SVM) models for protecting the financial sector from cybercrime; Wahid S. D. M., Buja A. G., [38] propose the application of an assessment model for assessing the influential factors of cyber security awareness; Buja A. G., Wahid S. D. M.[5] developed a model of cybersecurity awareness for the elderly.

So, at present, an acute and insufficiently researched problem of the functioning of enterprises is the lack of complex, reliable, effective approaches to the assessment of the activities of business entities in terms of the policy of protection against financial cyberattacks.

Modeling is a method of researching any phenomena, processes or objects by building and analyzing their models. In a broad sense, modeling is one of the main categories of the theory of cognition and almost the only scientifically based method of scientific research of systems and processes of any nature in many spheres of human activity. Today, considerable attention is paid to modeling. Consider the main types of models (Figure 1.3).

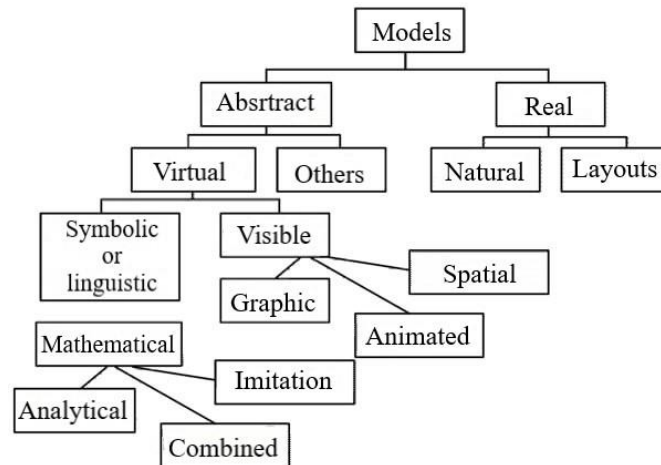


Figure 1. 3 – Main types of models

Visual models, depending on the method of implementation, can be divided into two- or three-dimensional graphic, animated and spatial models. Graphical and animated models are widely used to display the processes that occur in the modeled system. Graphical models are used in computer-aided design systems. To reproduce three-dimensional models using a computer, there are many graphic packages, the most common of which are: Corel DRAW, 3D Studio Mach and Maya. Graphical models are the basis of all computer games, and are also used during simulation modeling for animation.

An important component of assessing the functioning of enterprises is the modeling of the above-described due diligence processes.

1. Due diligence model based on machine learning [7] involves assessing the profitability of operations with problematic loans on the secondary market, modeling complex interrelationships between indicators; improving the due diligence process by developing an artificial intelligence algorithm. Such a model includes the following stages: the formation of a research base; modeling complex relationships between predictors and variables using ML algorithms; assessment of the profitability of transactions using due diligence; practical research and formation of opinions on the legislative framework for non-performing loans; forecasting the recovery level of the portfolio of secured problem loans based on the establishment of the regression

algorithm of the dependent random forest; dependent forest formation based on the application of non-linear canonical correlation (DF-NLCC); using a special division rule. At the same time, the classification and regression tree (CART) approach is the basis of cultivation. A criterion for the random division of the forest is proposed (formula 1.1):

$$K = \sqrt{VL * VR} * |rVL - rVR| \quad (1.1)$$

where K is the criterion for dividing the random forest; VL is the size of the left node; VR is the value of the right node; rVL is the value of the nonlinear canonical correlation estimate of the left node; rVR is the value of the non-linear canonical correlation estimate of the right node.

Next, the formulation of the approach to the pricing of the portfolio of problematic loans on the secondary market is carried out (formula 1.2):

$$VPPL = E[PVECF, i(0, t)] - CC, \quad (1.2)$$

Where VPPL is the value of the portfolio of problem loans on the secondary market; PVECF – present value of expected cash flows; CC – cost of capital; visualization of empirical application results.

2. Due diligence model based on risk assessment [31] provides a comprehensive methodology for performing due diligence of the risks of a multinational engineering and construction organization by third parties. The study of such risks includes: unscrupulous and illegal behavior of third parties, risks of integrity, violations of ethics and responsibility, propensity of the business model to risk, risks of corruption and bribery, risks of monopolization, competitive risks, human rights risks, risks of conflicts of interest, risks non-compliance with regulations. Development of a risk-adapted enterprise verification model, risk management mechanism.

3. Due diligence model based on deep active learning of NLP [1] provides for the formation of a model for proper verification and forecasting of the environment; adaptation and expansion of existing NLP natural language information processing models by adding environmental field data (EDD). The model includes the following stages: database formation; overcoming noise in the classification model by training the model to identify relevant things; overcoming the obstacles of uneven data collection through active learning, as well as expanding data. According to this technique, DistilBERT is configured on EDD data; the model is hosted as an application programming interface (API) on Hugging Face Hub; package, EnvBert, is hosted in the Python Package Index (PyPI) repository. The data set includes information: numerical recovery standards – concentrations of pollutants in the environment; the degree of contamination of the environment; water depth; interaction of underground and surface waters to detect environmental pollution; flow rate of water and pollutants; geological characteristics; contaminated environment – water, soil; restoration of the environment, elimination of pollution; recovery goals; sources of environmental pollution; dangerous environmental pollutants; irrelevant information.

4. NAP, mHRDD, BHR models of the optimality of the assessment of the implementation of the UN guidelines on business and human rights [27]. National Action Plans Model - a model of national action plans on business and human rights, a national political strategy taking into account the practices of states, which provides for a system of "soft" political instruments proposed by the government, describing the government's priorities, according to which future actions are aimed at facilitating the implementation of legal or implementation of political obligations regarding the verification of human rights, elimination of negative consequences of human rights as a result of economic activity. Mandatory Human Rights Due Diligence Model – mandatory model of human rights due diligence, which provides for "hard" legal decisions, legislative regulation of human rights due diligence through national legislation; acts of domestic legislation regarding to ensure compliance with

established standards of conduct by corporations Business and Human Rights Treaty Model – a model of the treaty on business and human rights, which provides for an international legally binding instrument on human rights for enterprises, depending on the areas of application.

5. A model of consensus multidimensional verification of investment projects based on financial technologies [25] involves a group approach to the evaluation of financial alternatives for investment projects. The model includes the following steps: determination of multidimensional factors of due diligence based on a balanced scorecard; analysis of group decision-making based on consensus (formation of the membership function, calculation of fuzzy preferences, calculation of levels of agreement, calculation of the global level of agreement of the formation of similarity matrices; determination of the global degree of consensus; determination of consensual degrees; calculation of collective fuzzy relations advantages; generation of levels of closeness and ratio between criteria; calculation of consensual control level); establishing directions of influence on financing alternatives based on the methodology of spherical fuzzy test sets; assessment of decision-making (DEMATEL) – calculation of the weight of various factors, development of a map of the relationship of influence (collection of expert evaluations; formation of a matrix of direct communication (formula 1.3):

$$X = \begin{bmatrix} 0 & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & 0 & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & 0 & \dots & x_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & x_{n3} & \dots & 0 \end{bmatrix} \quad (1.3)$$

where X is the direct connection matrix;

Normalization of the direct connection matrix (formula 1.4):

$$Y = \frac{X}{\max_{1 \leq i \leq n} \sum_{j=1}^n x_{ij}} \quad (1.4)$$

where U is the normalization of the matrix of the direct connection of the formation of the general matrix of the ratio.

6. A computer model of due diligence through AHP and big data [26] involves quantifying current technical due diligence. The model includes the following stages: formation of the research information base; data analysis based on the application of the 4C online evaluation method for corporate due diligence and decision-making (collection and formation of a single fund and database; determination of a comparison index, formation of a comparison matrix, evaluation of indicators at each level (while the technical evaluation model will have the form of a formula 1.5), performing consistency testing :

$$T = Aen * Ben + Aeq * Beq + Aes * Bes + Am * Bm \quad (1.5)$$

where T is the score of the technical evaluation model; Aen – equipment assessment, Aeq – environmental assessment, Aes – energy saving assessment, Am – management assessment;

calculation of task indicators and calculation of points (based on the method of conversion of the range for processing and three-level assessment); forming an assessment conclusion); analysis of the effect of implementation .

Considering the issue of modeling due diligence processes, let's focus on the current trends of this verification procedure in the aspect of modeling countering financial cyber fraud. Yes, the following models are worth a detailed look:

1. A model of the image of a victim of cybercrime [35] involves the creation of a phase image of a victim of a cybercrime based on the methods of systematization, comparison, grouping, logical generalization, bibliometric analysis, regression analysis (the method of sigma-limited parameterization), algorithm of associative rules. This model includes the following stages: formation of a base of indicators (selection of countries for analysis, selection of the research sector; selection of

informational features for research; selection of the most relevant indicators-characteristics of cyberfraud based on the application of sigma-limited parameterization (one-dimensional test significance), and construction of a Pareto diagram (visualization) of t-values for GRM coefficients; construction of a portrait of a victim of cyber fraud based on essential personal characteristics, which are calculated by using an algorithm of associative rules (implies the use of machine learning methods for data analysis to identify patterns in the database; use for analysis of the STATISTICA software product); forming conclusions on the most vulnerable categories of the population.

2. An econometric model of the impact of digitalization on economic transformations based on developed quantile regressions (taking into account the national cyber security indicator) [20]. This model provides for substantiating the existence of convergence processes in the direction of digitalization of countries, taking into account certain indicators the level of national cyber security, ease of obtaining electricity, ease of doing business, anti-money laundering index, level of digital development of the country. The model includes the following steps: preparation of the database for research, facilities (fixed broadband over 10 Mbps, mobile data and voice basket, high consumption), interference (enhanced broadband with 256 Kbps/ s to 2 Mbit/s and from 2 Mbit/s to 10 Mbit/s, basket of mobile data and voice, low consumption)); determination of sigma-convergence of digital processes using the coefficient of variation (formula 1.6) using indicators of digital development:

$$Kv = \frac{Sd}{m} * 100\% = \frac{\sqrt{\frac{\sum_{i=1}^n (a_i - m)^2}{(n - 1)}}}{\frac{\sum_{i=1}^n a_i}{n}} \quad (1.6)$$

where Kv – is the coefficient of variation, Sd – the standard deviation, m is the average value, n – the number of data points, a_i – the number of Internet users for the i -th country;

Development of a multiple regression model based on indicators for the model – the level of digital development of the country, the level of national cyber security, ease of obtaining electricity, ease of doing business, the Basel AML index, the development of quantile regression models, the formation of conclusions based on the model and indicators.

3. Linked machine learning (SVM) model for protecting the financial sector from cybercrime [17]. This model provides for the management of cyber security through the analysis of large volumes of data, which allows early detection and assessment of potential factors of cyber threats. The model contains relevant stages: formation of research hypotheses; collection of the statistical base of the study (selection of countries for the study; selection of indicators for characterizing the volume of cybercriminal operations – the share of mobile phones infected with malicious software, the share of computers attacked by phishing, the share of attacks by cryptominers, the share of countries targeted by malicious mailings, the share of users attacked by mobile banking trojans, the share of users attacked by extortion trojans, benefit- eyes attacked by mobile ransomware Trojans, share of all spam messages by country of origin, share of users attacked by banking malware, share of mobile users attacked via web sources, share of computers infected with at least one malicious attack, share of attacks via SSH by country of origin, share of telnet attacks by country of origin, share of computers subjected to at least one local malware attack); standardization of input indicators by the method of Z-normalization; construction of a single integral indicator using the Ivakhnenko data processing method (formula 1.7):

$$Ikn = \sum_{j=1}^j \sum_{j=1}^j (sn_j)^2 \quad (1.7)$$

where Ikn – the integral index of cyber threats in the section of the n th country, sn_j – the standardized value of the j – indicator of the spread of cyber threats in the section of the n th country;

Determination of potential factors of the spread of cyber threats; implementation of the construction of two types of SVM machine learning models, different types of functional dependence are built between by applying the reference vector method (formula 1.8):

$$f = \left\{ \begin{array}{ll} a_i * a_j & \text{linear type} \\ \exp(-h * (a_i - a_j)^2) & \text{radial basis type} \\ (h * a_i * a_j + c)^p & \text{polynomial type} \\ \tanh(h * a_i * a_j + c) & \text{sigmoid type} \end{array} \right\} \quad (1.8)$$

where f is the functional dependence between variables, a – the independent variable, p is the degree of the polynomial kernel, h – the gamma parameter for polynomial, radial, and sigmoid kernels, c – the coefficient for polynomial and sigmoid kernels); generalization of research results.

4 Scoring Models for Assessing the Influential Factors of Cybersecurity Awareness [38] involves a quantitative study of factors of organizational, social and individual influence on cyber security awareness. This model includes the following stages: formation of a statistical research base (formation of a demographic profile, a group of people of a certain age is selected using a convenient sampling technique; factors are selected - organizational, social and individual influence on cyber security awareness); data measurement model testing; testing structural model (hypothesis testing), CMV (common method variance) testing, formation of research conclusions.

5. A Cybersecurity Awareness Model for Seniors [5] involves the development of an organizational, social and individual cyber security awareness model (Osicsam) for the elderly. The model includes the following sequential steps: feasibility study and literature review of cybersecurity awareness and learning styles of older adults; existing approaches to cyber security awareness are analyzed in detail; learning styles were studied, taking into account the peculiarities of the elderly; general models of awareness of cyber security are compared with the peculiarities of the education of older people; mapping was carried out; a cyber security awareness model for the elderly was developed the model was formed on the basis of the model of information security awareness opportunities, the general model of the information security awareness program, the peer education model, the security awareness model; analysis of the effectiveness of the model and based on expert reviews.

The implementation of a comprehensive Due Diligence methodology in the aspect of countering financial cyber fraud will contribute to the provision of the following advantages for enterprises:

- improvement of corporate management, improvement of the regulatory framework of corporate management; formation of effective business solutions;
- ensuring long-term sustainability and stability; formation of resilience in chains of continuous activity to sudden threats; obtaining competitive advantages;
- avoiding unwanted reputational risks; reduction of value creation risks; mitigation of risks; reduction of losses from business activities;
- strengthening of corporate responsibility for adverse consequences of doing business;
- formation of agreement among enterprises regarding obligations according to norms of enterprise activity;
- provision of better legal protection for enterprises affected by the functioning of enterprises; improvement of enterprise security policy.

1.3. Statement of the modeling problem and formulation of model requirements

Before the mathematical description of the model and performing calculations, it is necessary to form a general scheme that will reflect the research mechanism.

Modeling will be carried out at the macro level in the cross-section of the selected indicators for the countries of the world. During modeling, the most significant quantitative characteristics of the research object were selected. The research period is proposed to be 2021 (actual data from global open sources).

The model must meet the following criteria:

1. To take into account the nominal values of the selected indicators, which determine the state of combating financial cyber fraud in the countries of the world;
2. Allow mapping of input data;
3. Take into account the relevance of factor indicators that determine the state of combating financial cyber fraud;
4. To take into account the statistical significance of factor indicators that determine the state of combating financial cyber fraud.
5. Take into account the strength of influence, as well as the direction of influence of the identified relevant factors on the level of cyber security.
6. Provide an economic-mathematical interpretation of the constructed multiple linear regression
7. Adequacy criteria given at certain stages of the model.
8. Correspond to the normal law of distribution.

Therefore, the model should adequately reflect the level of the studied volumes and meet such criteria as reliability, efficiency, control over results, expediency of the management level and systematicity.

Model calculations will be carried out with the help of MS Excel spreadsheet processor, Statistica statistical package. These programs are easy to use, and thanks to the built-in functions, the research tools will facilitate the process of design calculations.

Thus, the task of this study is to develop a mathematical model for determining the economic and mathematical modeling of due diligence of enterprises as of 2021.

1.4. Mathematical model development

The determination of the relevant factors affecting the level of cyber security of the group of indicators characterizing the state of combating financial cyber fraud for the countries of the world is implemented in 4 stages.

At the first stage of the research, the statistical base of the study is collected, which characterizes the state of combating financial cyber fraud; selection by countries of the world of factors affecting the state of cyber security. The research information base is built on the basis of indicators of The World Bank, Global Digital Convergence, Digital Development Dashboard, NCSI. Evaluation indicators were selected for 2021 for 68 countries of the world. Thus, the following 32 indicators Digital Development Level (C1), Basel AML Index (C2), Assessment of the ease of doing business (C3), Assessment of the ease of obtaining electricity (C4), Human Development Index(C5), Index Distribution of human rights(C6), Secure Internet servers (C7), Business extent of disclosure index (0=less disclosure to 10=more disclosure) (C8), Research and development expenditure (% of GDP) (C9), Firms competing against unregistered firms (% of firms) (C10), Firms using banks to finance working capital (% of firms) (C11), Firms that spend on R&D (% of firms) (C12), Losses due to theft and vandalism (% of annual sales of affected firms) (C13), Firms offering formal training (% of firms) (C14), Firms experiencing losses due to theft and vandalism (% of firms) (C15), Informal payments to public officials (% of firms) (C16), Firms using banks to finance investment (% of firms) (C17), Value lost due to electrical outages (% of sales for affected firms) (C18), Fixed broadband subscriptions: >10 Mbit/s (C19), Individuals using the Internet, total (%) (C20), Active mobile-broadband subscriptions per 100 inhabitants (C21), Fixed

broadband basket as a % of GNI p.c. (C22), Fixed broadband subscriptions per 100 inhabitants (C23), Fixed-telephone subscriptions per 100 inhabitants (C24), Mobile broadband basket as a % of GNI p.c. (C25), Mobile cellular basket as a % of GNI p.c. (C26), Mobile data and voice basket (high consumption) as a % of GNI p.c. (C27), Mobile data and voice basket (low consumption) as a % of GNI p.c. (C28), Mobile-cellular subscriptions per 100 inhabitants (C29), Population covered by a mobile-cellular network (%) (C30), Population covered by at least a 3G mobile network (%) (C31) Total fixed broadband subscriptions (C32). The National Cyber Security Index (C0) is used as the effective indicator of the level of cyber security.

At the second stage, a cluster analysis was carried out – the grouping of the countries of the world into clusters using the tools of the Statistica 10 and Statistica Portable programs. Clustering of countries is based on the application of the iterative divisive method of k-means (k-means clustering). For further clustering of countries, a statistical base of indicators from 33 indicators for 68 countries of the world was initially selected. Then, with the help of cluster analysis, the adequacy of the division of countries into groups was checked. To evaluate and compare clusters, variance analysis was used to select clusters. That is, with the help of dispersion analysis, the expediency of grouping countries according to the level of cyber security and the state of combating financial cyber fraud into 9 clusters has been proven. For this purpose, the value of the intragroup (minimized) and intergroup (maximized) variance of the characteristics is determined, as well as the parameters F (Fisher's criterion – should be more than critical) and p (the probability of rejecting the hypothesis about the inexpediency of a certain grouping – goes to 0, for economic research it should be less than 0,05). Thus, the results of grouping from 2 to 12 clusters were considered sequentially.

Dispersion analysis is a set of statistical methods designed to test hypotheses about the relationship between a certain characteristic and the investigated factors that do not have a quantitative description, as well as to establish the degree of influence of factors and their interaction.

In univariate analysis of variance, the output data is presented in the form of a table in which the number of columns is equal to the number of factor levels, and the number of values in each column is the number of observations at the corresponding factor level. (table 1.2) For different levels of the factor, the number of observations may be different. At the same time, it is assumed that the results of observations for different levels are samples from normally distributed populations, the average value and variance of which are the same and do not depend on the levels. The task of the analysis is to test the null hypothesis about the level of the average values of the populations under consideration.

Table 1.2 – The form of the table of observations when conducting one-factor variance analysis

Measurement results	Factor levels			
	1	2	...	k
1	a ₁₁	a ₁₂	...	a _{1k}
2	a ₂₁	a ₂₂	...	a _{2k}
...
n _i	a _{ni1}	a _{ni2}	...	a _{nik}

The method is based on the identity of variance analysis, according to which the sum of the squared deviations of observations from the general mean (general variation) is equal to (formula 1.9):

$$\sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \bar{a})^2 = \sum_{j=1}^k n_j (\langle a_j \rangle - \bar{a})^2 + \sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \langle a_j \rangle)^2 \quad (1.9)$$

$$\bar{a} = \frac{1}{N} \sum_{j=1}^k \sum_{i=1}^{n_j} a_{ij} - \text{overall average; } \langle a_j \rangle = \frac{1}{n_j} \sum_{i=1}^{n_j} a_{ij} \quad j = 1, \dots, k;$$

$$N = \sum_{j=1}^k n_j - \text{total number; } k - \text{number of samples; } n_j$$

(j=1,2, ..., k) – the number of elements y j samples; $\langle a_j \rangle$ – average value j-ï samples.

In the right part (formula 1.10) of the first appendix (factorial or intergroup variation) is the weighted sum of squared deviations of the average groups from the overall average. It characterizes the fluctuations of values caused by the factor on the basis of which the grouping of data was carried out. the second supplement (residual, or within-group variation) is the sum of the squared deviations of the observations and the corresponding group means. It characterizes fluctuations in the values of the investigated characteristic caused by unaccounted for or random factors.

The essence of the method is that if the null hypothesis is true, the value (formula 1.10, 1.11):

$$\sigma_2^2 = \frac{1}{N-1} \sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \langle a_j \rangle)^2 \quad (1.10)$$

So

$$\sigma_2^2 = \frac{1}{k-1} \sum_{j=1}^k n_j (\langle a_j \rangle - \bar{a})^2 \quad (1.11)$$

are unbiased estimates of the observation errors σ^2 and should be approximately equal to each other. The first of them is a measure of variation within samples and is not related to the assumption of equality of mean values, therefore $\sigma^2 \approx \sigma_1^2$ regardless of the validity of the null hypothesis. The second estimate characterizes the variation between samples. If the null hypothesis is correct, $\sigma_2^2 \approx \sigma^2$, and if it is violated, the value of σ_2^2 is greater the greater the deviation from it.

The value of Fisher's criterion is calculated according to the formula (1.12):

$$F = \frac{(N-k) \sum_{j=1}^k n_j (\langle a_j \rangle - \bar{a})^2}{(k-1) \sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \langle a_j \rangle)^2} \quad (1.12)$$

This quantity has Fisher's F-distribution with parameters $k-1$ and $N-k$. The null hypothesis is rejected if the probability $P(F \geq F^*)$, where the F^* -value calculated from empirical data using formula (3) is small enough.

At this stage, the Statistica toolkit, the package "Multivariate Exploratory Techniques" – "Canonical Analysis" – k-means clustering – analysis of variance – was used for dispersion analysis; "Multivariate Exploratory Techniques" – "Canonical Analysis" – k-means clustering – Member of each clusters – to directly distinguish certain groups of countries that are typical for their characteristics.

At the third stage of the research of this factor analysis, relevant factors characterizing the state of combating financial cyber fraud for the countries of the world are presented, using the methods of sigma-limited parameterization and correlation analysis.

The third stage of the research was conducted using Statistica 10 and . Portable statistics. At this stage, the "Statistics" toolkit, the package "Advanced Linear/Nonlinear Models" General Regression Models" – "General linear models" are used. The implementation of this stage includes conducting one-factor tests of the significance of factors characterizing the state of countermeasures against financial cyber security and the construction of a Pareto t-value diagram of the significance of the influence of factors that determine the state of countermeasures against financial cyber fraud (rules of graphic visualization 80 by 20), taking into account the obtained in the general regression model of the connection between the selected factors of the state of combating financial cyber fraud and the level of cyber security. We look for statistical significance, focusing on the critical permissible value of Fisher's test (p) 0.05 (the indicator should be less than 0.05), as well as on the highest levels of sums of squared deviations (SS).

Within the framework of the third stage – establishing for the countries of the world relevant factors that determine the state of combating financial cyber fraud affecting cyber security, it is also necessary to conduct a correlation analysis.

The statistical method used to study relationships is called correlation analysis. The absolute value (module) of a special indicator - the correlation coefficient – is used to assess the closeness of the relationship in the correlation analysis. The absolute value of the correlation coefficient is in the range from 0 to 1. The correlation coefficient gives several estimates of the statistical relationship between the measurement results.

To assess the statistical relationship, when the measurement is carried out in the school of ratios or intervals and the form of the relationship is linear, the Brave-Pearson correlation coefficient is used, which is calculated as follows (formula 1.13):

$$r = \frac{\sum_{i=1}^n (a_i - \bar{a})(b_i - \bar{b})}{\sqrt{\left[n \sum_{i=1}^n a_i^2 - \left(\sum_{i=1}^n a_i \right)^2 \right] \left[n \sum_{i=1}^n b_i^2 - \left(\sum_{i=1}^n b_i \right)^2 \right]}} \quad (1.13)$$

At this stage, the "Statistics" toolkit, the "Basic Statistics/Tables" – "Correlation matrices" package are used. The implementation of this stage includes the construction of a correlation matrix of interdependence of important factors that determine the state of combating financial cyber fraud. The correlation coefficients calculated in the correlation matrix between the performance indicator, as well as separately between the factor cyber security indicators, describe the strength of the connection between the selected features: strong connection – the value of the correlation coefficients is greater than 0.7, medium connection – the value of the correlation coefficients from 0, 4 to 0.7, weak connection – the value of correlation coefficients from 0.1 to 0.4.

At the fourth stage of the study, the strength of influence and the direction of influence of relevant factors selected for the countries of the world, which determine the state of combating financial cyber fraud, are determined. Within this stage, a multiple linear regression is constructed using the method of least squares – the OLS method.

A function that reflects the statistical relationship between features is called a regression equation.

In the regression equation of statistical dependence, X is called the regression coefficient, Y is the free term of the regression.

The value of the regression coefficient is calculated by solving the system of normal equations (formula 1.14):

$$\begin{cases} nx + y \sum a = \sum b \\ x \sum a + y \sum a^2 = \sum ab \end{cases} \quad (1.14)$$

$$\begin{cases} a_1 \\ a_2 \\ \dots \\ a_m \end{cases} \text{ незалежні фактори} \rightarrow \text{B залежний фактор}$$

The multiple regression model is an equation that expresses the correlation between the result in several factors (formula 1.15):

$$B = f(a_1, a_2, \dots, a_m) \quad (1.15)$$

The most common method of estimating unknown regression parameters on a sample data model is the ordinary least squares method. The essence of the method is that the parameters of the function (), with the help of which the approximation is carried out, determined in accordance with the condition of minimizing the sum of squares of the model errors, namely the sum of squares of the difference between the empirical values of the internal factor and those calculated according to the econometric model (formula 1.16):

$$F(\theta^*) = \sum_{i=1}^n \varepsilon_i^2 = \sum_{i=1}^n (b_i - \bar{b}_i)^2 \rightarrow \min \quad (1.16)$$

де b_i – the value of the internal factor by which the measurement was obtained;

\hat{b}_i – the estimated value of the internal factor, which is calculated according to the econometric model in the case of substitution of values and external factors corresponding to its measurement in this model;

n – the size of the sample population;

$F(\theta^*)$ – the sum of squares of the model errors, which is a function of the video estimates of the model parameters.

The fourth stage of the research was conducted using Statistica 10 and Statistica Portable programs. At this stage, the "Statistics" toolkit, the "Multiple regression" – "Summary regression" package were applied. As a result, we obtain in tabular form the calculated indicators of the regression analysis of the dependence between the factors that determine the state of combating financial cyber fraud, as well as between cyber security relevant, statistically significant factors of cyber fraud, based on the data of which a multiple linear regression of the dependence between the factors that determine the state of combating financial fraud cyber frauds, as well as a multiple linear regression of the dependence between organizational cyber security and the corresponding relevant, statistically significant factors.

An analysis of the linear multiple regression model was carried out between the factors that determine the state of combating financial cyber fraud, for which, among other things, a graph of compliance with the normal law of the distribution of the residuals of the linear regression model of cyber security dependence was additionally constructed in the Statistica 10 and Statistica Portable programs (the graph was constructed using the "Statistics" toolkit ", package "Multiple regression" – "Residuals/assumptions/prediction" – "Perform analysis of residuals" – "Normal plot of residuals").

Taking into account the stages described above, we will build a generalized scheme of economic and mathematical modeling (figure 1.4).

Incoming data	Mathematical ratio	Output variables
C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, C14, C15, C16, C17, C18, C19, C20, C21, C22, C23, C24, C25, C26, C27, C28, C29, C30, C31, C32	$\sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \bar{a})^2 = \sum_{j=1}^k n_j (\langle a_j \rangle - \bar{a})^2 + \sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \langle a_j \rangle)^2$ $F = \frac{(N - k) \sum_{j=1}^k n_j (\langle a_j \rangle - \bar{a})^2}{(k - 1) \sum_{j=1}^k \sum_{i=1}^{n_j} (a_{ij} - \langle a_j \rangle)^2}$ $r = \frac{\sum_{i=1}^n (a_i - \bar{a})(b_i - \bar{b})}{\sqrt{[n \sum_{i=1}^n a_i^2 - (\sum_{i=1}^n a_i)^2][n \sum_{i=1}^n b_i^2 - (\sum_{i=1}^n b_i)^2]}}$ $nx + y \sum a = \sum b$ $x \sum a + y \sum a^2 = \sum ab$ $B = f(a_1, a_2, \dots, a_m)$ $F(\theta^*) = \sum_{i=1}^n \varepsilon_i^2 = \sum_{i=1}^n (b_i - \hat{b}_i)^2 \rightarrow \min$	$\bar{a} = \frac{1}{N} \sum_{j=1}^k \sum_{i=1}^{n_j} a_{ij} - \text{overall average;}$ $\langle a_j \rangle = \frac{1}{n_j} \sum_{i=1}^{n_j} a_{ij} \quad j = 1, \dots, k;$ $N = \sum_{j=1}^k n_j - \text{total number;}$ $k - \text{number of samples; } n_j$ $(j=1, 2, \dots, k) - \text{the number of elements y j samples;}$ $\langle a_j \rangle - \text{average value j-i samples.}$
	Controlled variables Number of clusters	

Figure 1. 4 – Generalized scheme of economic and mathematical modeling

CHAPTER 2. VERIFICATION OF THE ADEQUACY OF THE MODEL AND PROPOSALS FOR ITS USE

2.1. Checking the adequacy of the constructed mathematical model

First, the adequacy of the model was tested at stage 2 (cluster analysis) using analysis of variance. The expediency of grouping the countries of the world according to the state of countering financial cyber fraud and the level of cyber security into 9 clusters, taking into account the value of intra-group and inter-group dispersion of characteristics, parameters F (Fisher's criterion), parameters p (probability of rejecting the hypothesis that a certain grouping is not appropriate) has been proven. Thus, the results of grouping from 2 to 12 (Figures 2.1, B.1 – B.5) clusters were considered sequentially.

According to the results of dispersion analysis, we observe an improvement in adequacy indicators when moving to 9 groups, followed by their deterioration when clustering from 10 groups. This is explained by the fact that when selecting from 2 to 8 clusters in terms of most input indicators, the following values of adequacy indicators are observed: different from zero value of intergroup variance (which contradicts the requirement to minimize this variance); in the cross-section of the intergroup variance, values close to zero are observed in most cases; low values of the Fisher test; p values are greater than 0.05 in a section of a number of indicators. This indicates the impracticality of grouping into 2-8 clusters.

The situation improves significantly when switching to 9 clusters (Figure 2.1). In comparison with figures B.1 – B.5, the values of intergroup variance generally increase, intragroup variance decreases, and most of the input indicators are statistically significant (23 out of 33 indicators – the p values for which approach the permissible level of less than 0.05, and 10 statistically insignificant: C1, C8, C11, C12, C13, C14, C15, C16, C17, C31).

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,524654E+0	8	2,269475E+0	59	4,955	0,00010
C1	7,809341E+0	8	9,885562E+0	59	5,826	0,00001
C2	3,094147E+0	8	5,735105E+0	59	3,975	0,00080
C3	7,134303E+0	8	7,775247E+0	59	6,767	0,00000
C4	7,134303E+0	8	7,775247E+0	59	6,767	0,00000
C5	5,845594E-0	8	6,596292E-0	59	6,536	0,00000
C6	6,455577E-0	8	2,742421E+0	59	1,736	0,10890
C7	3,373626E+1	8	9,425740E+1	59	2,640	0,01522
C8	7,848264E+0	8	3,136927E+0	59	1,845	0,08650
C9	2,279906E+0	8	5,870506E+0	59	2,864	0,00924
C10	8,750300E+0	8	2,226524E+0	59	2,895	0,00857
C11	1,506828E+0	8	1,244834E+0	59	0,893	0,52841
C12	1,398658E+0	8	6,815490E+0	59	1,513	0,17210
C13	1,089695E+0	8	7,119233E+0	59	1,125	0,35776
C14	4,195098E+0	8	1,850678E+0	59	1,672	0,12452
C15	1,853194E+0	8	6,759950E+0	59	2,022	0,05921
C16	6,100735E+0	8	2,286789E+0	59	1,965	0,06657
C17	1,148288E+0	8	1,595149E+0	59	0,531	0,82853
C18	6,337980E+0	8	2,081157E+0	59	2,246	0,03631
C19	2,770574E+1	8	2,909506E+1	59	7022,83	0,00000
C20	1,458598E+0	8	1,449012E+0	59	7,424	0,00000
C21	2,466829E+0	8	4,567978E+0	59	3,983	0,00079
C22	1,158186E+0	8	1,963262E+0	59	4,351	0,00036
C23	5,251958E+0	8	8,636795E+0	59	4,485	0,00027
C24	3,765020E+0	8	1,154849E+0	59	2,404	0,02562
C25	6,424162E+0	8	6,297721E+0	59	7,523	0,00000
C26	2,968103E+0	8	3,259851E+0	59	6,715	0,00000
C27	1,401115E+0	8	1,248847E+0	59	8,274	0,00000
C28	4,109352E+0	8	2,922943E+0	59	10,365	0,00000
C29	1,114735E+0	8	3,332745E+0	59	2,467	0,02232
C30	2,985987E+0	8	9,115524E+0	59	2,416	0,02498
C31	1,658097E+0	8	6,534629E+0	59	1,871	0,08181
C32	2,809651E+1	8	3,303997E+1	59	6271,54	0,00000

Figure 2.1 – Analysis of the adequacy of the clustering of the countries of the world into 9 groups as of 2021

When transitioning from 10, and then 11 to 12 clusters, the indicators of grouping adequacy according to the results of dispersion analysis deteriorate again (Figure B.1 - B.5). We observe that the probability of rejecting the hypothesis about the inappropriateness of this grouping is greater than the permissible level of 0.05 for most of the input indicators. Thus, it is possible to draw a conclusion about the expediency of grouping the countries of the world into 9 clusters according to the state of combating financial cyber fraud and cyber security.

Secondly, the adequacy of the model was checked at stage 3 (identification of relevant factors that determine the state of combating financial cyberfraud, when conducting Univariate Tests of Significance (Figure 2.10)). Adequacy was checked using indicators of variance analysis as in the 2nd stage; as well as by constructing a Pareto Chart of t-Values of the significance of the influence of factors determining

the state of combating financial cyber fraud on the level of cyber security (Figure 2.11).

Thirdly, the adequacy of the model was checked at stage 4 (determination of the strength and direction of influence of relevant factors, construction of multiple linear regression). The adequacy of the regression analysis model was checked using adequacy indicators (the coefficient of determination and Fisher's test value) for 68 countries of the world for 32 factors, for 68 countries of the world for 5 factors, for 68 countries of the world for 4 factors (Figure B.6, Figure B.8 , Figure 2.2). Also, the accuracy and adequacy of the model is confirmed by constructing a graph of compliance with the normal law of the distribution of the residuals of the linear regression model of dependence between the level of cyber security of relevant factors that determine the state of combating financial cyber fraud in 68 countries of the world for 32 factors, in 68 countries of the world for 5 factors, in 68 countries of the world for 4 factors (Figure B.7, Figure B.9, Figure 2.3).

The model for 68 countries of the world for 32 factors is not sufficiently adequate and accurate in view of the corresponding level of the coefficient of determination of 0.9056 (corresponds to the norm) and the value of the Fisher criterion of 20.89 (does not correspond to the critical value) (Figure B.6), which is less than the critical permissible level); the model for 68 countries of the world for 5 factors is sufficiently adequate and accurate in view of the corresponding level of the coefficient of determination of 0.8754 (corresponding to the norm) and the value of the Fisher criterion of 40.6784 (corresponding to the critical value), which is more than the critical permissible level; for 68 countries of the world for 4 factors - is fully adequate and accurate in view of the corresponding level of the coefficient of determination of 0.8720 (corresponding to the norm) and the value of the Fisher criterion of 50.0224 (corresponding to the critical value), which is more than the critical permissible level. (Figure 2.2, formula 2.2).

Summary Statistics; DV: C0 (SpreadsheetBerezhna_fa	
Statistic	Value
Multiple R	0,87209
Multiple R?	0,76052
Adjusted R?	0,74532
F(4,63)	50,0224
p	0,00000
Std.Err. of Estimate	12,0089

Figure 2.2 – Indicators of the adequacy of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud for 68 countries of the world (4 factors)

According to Figure B.7 for 68 countries of the world for 32 factors, it can be seen that the residuals of the linear regression model of dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud do not fully correspond to the normal distribution law; Figure B.9 for 68 countries of the world for 5 factors - the residuals of the linear regression model of dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud sufficiently correspond to the normal distribution law; Figure 2.3 for 68 countries of the world for 4 factors - the residuals of the linear regression model of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud fully corresponds to the normal distribution law.

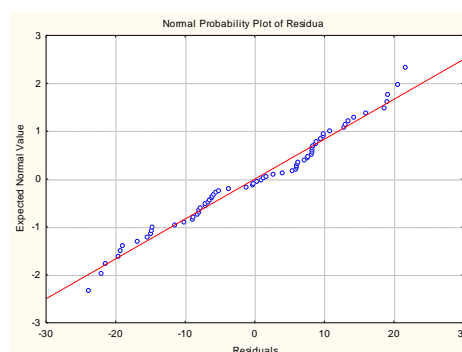


Figure 2.3 – Graphic representation of compliance with the normal law of the distribution of the residuals of the linear regression model of the dependence between

the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for 68 countries of the world (4 factors)

Similarly, the adequacy and accuracy of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud for the cluster with Ukraine was checked for 32 factors (Figure B.10) - the model is completely inadequate, and 5 factors (Figure Figure 2.4, formula 2.3) – the model is adequate and accurate in view of the corresponding level of the coefficient of determination 0.9932 (corresponds to the norm) and the value of the Fisher criterion 14.7133 (corresponds to the critical value), which is more than the critical permissible level.

Summary Statistics; DV: C0 (SpreadsheetBerezhna_fact_cl3	
Statistic	Value
Multiple R	0,99327
Multiple R?	0,98659
Adjusted R?	0,91955
F(5,1)	14,71330
p	0,19528
Std.Err. of Estimate	4,90500

Figure 2.4 – Indicators of the adequacy of the regression analysis of the dependence between the level of cyber security and the factors determining the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (5 factors)

According to Figure 2.5, it can be seen that the residuals of the linear regression model of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (5 factors) correspond to the normal distribution law.

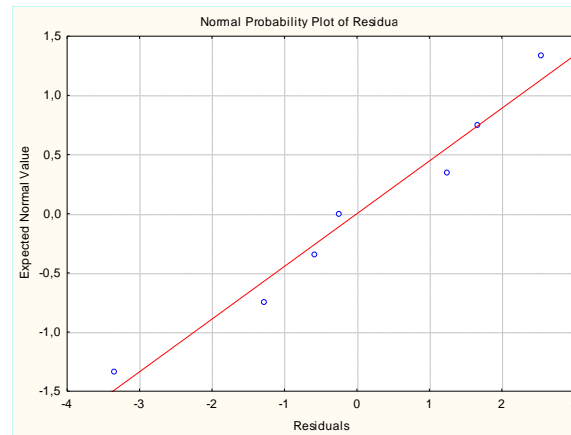


Figure 2.5 – Graphic representation of compliance with the normal law of the distribution of the residuals of the linear regression model of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (5 factors)

2.2. Construction of the methodology of design calculations

Stage 2. Formation of the input statistical base. To perform quantitative formalization, statistical data for 2021 was prepared for 68 countries of the world based on 33 indicators from The World Bank, Global Digital Convergence, Digital Development Dashboard, NCSI. Input data is formed in table 2.1.

Stage 2. Cluster analysis. The second stage was a cluster analysis using the k-means clustering method. On the basis of the formed input base of 33 indicators for the year 2021 for 68 countries of the world, taking into account the dispersion analysis described in point 1.4 and point 2.1, the grouping of the countries of the world into 2 to 12 clusters was performed (Figure 2.1, B.1 – B .5); the expediency of grouping the countries of the world into 9 clusters has been proven.

Table 2.1 – Fragment of quantitative formalization of the statistical base of the study

Country	C0	C1	C2	...	C30	C31	C32
Albania	62,3400	48,7400	5,7200	...	99,8600	99,2000	559394,0000
Austria	68,8300	75,7600	4,4200	...	99,0000	98,0000	2592000,0000
Belarus	53,2500	62,3300	5,0400	...	99,9000	99,9000	3238881,0000
Belgium	94,8100	74,0700	3,9400	...	100,0000	100,0000	4920679,0000
Botswana	29,8700	41,9600	4,8700	...	98,0000	98,0000	203020,0000
Bulgaria	74,0300	62,0600	5,1600	...	99,9900	99,9900	2253977,0000
Cambodia	15,5800	34,5900	7,1300	...	99,6000	95,7000	336243,0000
Cameroon	32,4700	28,2800	6,8800	...	79,8900	25,8000	579594,0000
...
Tunisia	53,2500	46,2600	5,2000	...	99,0000	99,0000	1496897,0000
Türkiye	54,5500	58,2900	5,7000	...	99,7500	98,8100	18135736,0000
Ukraine	75,3200	55,9600	5,2100	...	99,9000	91,6000	7566286,0000
Uruguay	59,7400	63,8600	3,9800	...	92,7000	92,7000	1105458,0000
Uzbekistan	36,3600	49,0000	5,2000	...	99,4000	95,0000	7497459,0000
Vietnam	36,3600	47,6900	7,0400	...	99,8000	99,8000	19328191,0000
Zambia	55,8400	29,6600	6,0300	...	97,1000	95,5000	80592,0000
Zimbabwe	15,5800	28,9700	6,7900	...	93,5400	84,3100	205333,0000

Thus, 9 separate clusters were determined (Figure 2.6, B.11, B.12), which contain the grouping of the countries of the world according to the selected key indicators in graphic form, indicating the number of member countries of each cluster, Euclidean distances from the center grouping as a determining indicator of this type of grouping of the countries of the world.

Members of Cluster Number 3 (SpreadsheeBerezhna_clast_t.s) and Distances from Respective Cluster Center Cluster contains 7 cases	
	Distance
Colombia	441835,0
Egypt	432249,0
Indonesia	494527,0
Netherlands	547481,0
Poland	354955,0
Thailand	742940,0
Ukraine	434756,0

Figure 2.6 – Composition and characteristics of the 3rd out of 9 conditional clusters of countries of the world in terms of the level of cyber security and the state of combating financial cyber fraud according to the Euclidean distance indicator

The analysis of the formed clusters of the countries of the world allows us to assert that the grouping fully corresponds to the general level of cyber security and the state of combating financial cyber fraud in the countries of the same cluster. Thus, a cluster of countries containing Ukraine, which was selected for research in the work, was singled out for further analysis. That is, this cluster includes Colombia, Egypt, Indonesia, the Netherlands, Poland, Thailand, Ukraine - countries that share common features of cyber security and the state of combating financial cyber fraud.

A more comprehensive description of the results of the cluster analysis allows the analysis of indicators using standardized average values (Figure 2.7) and Euclidean distances (Figure 2.8).

Variable	Cluster Means (SpreadsheetBerezhna_clust_t.sta)								
	Cluster No. 1	Cluster No. 2	Cluster No. 3	Cluster No. 4	Cluster No. 5	Cluster No. 6	Cluster No. 7	Cluster No. 8	Cluster No. 9
C0	65	52	66	78	65	55	47,7	42,4	28,1
C1	63	62	58	66	61	53	51,0	53,1	28,7
C2	5	7	5	4	5	5	5,5	5,7	6,6
C3	85	95	81	85	79	82	74,9	72,3	51,3
C4	85	95	81	85	79	82	74,9	72,3	51,3
C5	1	1	1	1	1	1	0,8	0,8	0,5
C6	1	0	1	1	1	1	0,7	0,8	0,7
C7	247654	196299	75807	35233	47190	21965	22386,6	14255,4	1930,6
C8	7	10	9	7	7	6	5,6	5,6	6,2
C9	1	3	1	2	2	1	0,6	0,4	0,2
C10	28	58	43	29	37	52	43,3	50,2	65,2
C11	37	22	32	33	35	34	26,2	39,2	25,5
C12	15	39	11	16	18	15	6,9	12,8	10,7
C13	3	1	3	3	4	4	3,6	4,6	6,8
C14	29	79	27	38	36	34	24,7	41,9	28,9
C15	16	4	11	19	13	16	9,7	19,6	26,7
C16	21	11	13	6	12	3	15,7	16,4	38,1
C17	36	15	30	31	33	28	23,2	30,3	25,4
C18	2	1	1	1	5	1	1,5	2,5	10,6
C19	2103371	53187470	875453	385156	186338	103367	543886,3	281473,3	15436,4
C20	82	73	78	86	80	78	72,7	75,9	35,1
C21	92	102	112	103	103	97	81,5	85,1	44,8
C22	2	1	3	2	3	5	5,4	6,1	43,9
C23	29	38	19	33	23	20	15,4	20,8	1,3
C24	26	13	12	26	17	17	15,1	20,9	0,9
C25	1	1	1	1	1	1	1,9	2,4	10,6
C26	1	0	1	1	1	1	1,1	1,9	7,4
C27	1	1	2	1	2	2	2,8	5,3	15,8
C28	1	1	1	1	1	1	1,8	3,1	8,7
C29	120	122	134	119	127	132	108,5	120,3	89,4
C30	99	100	99	100	98	98	98,8	96,9	92,6
C31	99	100	98	98	96	98	98,2	90,9	83,4
C32	2232355	53578660	971010	452984	237630	98789	756578,1	375129,1	101240,4

Figure 2.7 – Average values of indicators of the level of cyber security and the state of combating financial cyber fraud within 9 clusters

The smaller the value of the Euclidean distance, the more similar the countries in this cluster are in terms of the level of cyber security and the state of combating financial cyber-fraud.

Euclidean Distances between Clusters (SpreadsheetBerezhna_clast_t.xls)									
Cluster Number	Distances below diagonal								
	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8	No. 9
No. 1	0	1,589706E+1	9,479705E+1	1,867740E+1	2,331553E+1	2,609807E+1	2,699969E+1	2,783185E+1	2,853704E+1
No. 2	12608360	0,000000E-0	1,667917E+1	1,700136E+1	1,713457E+1	1,720623E+1	1,722950E+1	1,725032E+1	1,726779E+1
No. 3	307891	1,291479E+0	0,000000E-0	1,546629E+1	3,071346E+1	4,128194E+1	4,488533E+1	4,832963E+1	5,129510E+1
No. 4	432173	1,303892E+0	1,243636E+0	0,000000E-0	2,607549E+1	6,240928E+1	7,662778E+1	9,127741E+1	1,043977E+1
No. 5	482861	1,308991E+0	1,752526E+0	5,106417E+0	0,000000E-0	8,541027E+1	1,383836E+1	2,035331E+1	2,670214E+1
No. 6	510862	1,311725E+0	2,031796E+0	7,899954E+0	2,922503E+0	0,000000E-0	8,890928E+0	2,852581E+1	5,525368E+1
No. 7	519612	1,312612E+0	2,118616E+0	8,753730E+0	3,719994E+0	9,429172E+0	0,000000E-0	6,497887E+0	2,148926E+1
No. 8	527559	1,313405E+0	2,198400E+0	9,553921E+0	4,511464E+0	1,688958E+0	8,060947E+0	0,000000E-0	4,422498E+0
No. 9	534200	1,314070E+0	2,264842E+0	1,021752E+0	5,167411E+0	2,350610E+0	1,465921E+0	6,650187E+0	0,000000E-0

Figure 2.8 – Euclidean distances between 9 clusters

Stage 3 – Determination of the relevant (most influential) factors for the countries of the world that determine the state of combating financial cyber fraud, affecting the level of cyber security, based on Sigma-restricted parameterization and correlation analysis techniques.

The first step of the third stage is the performance of Univariate Tests of Significance of factors that determine the state of combating financial cyber fraud at the level of cyber security (Figure 2.9).

According to the data in Figure 2.9, which reflect the results of Univariate Tests of Significance of the influence of the factors that determine the state of combating financial cyber-fraud on the level of cyber security, 3 statistically significant factors were selected: C2, C19, C32. As for these factors, the calculated level of significance of Fisher's criterion meets the requirement - less than the critically permissible $p=0.05$ (for C2 - $p=0.00901$, C19 - $p=0.03184$, C32 - $p=0.03206$); the highest levels of sums of squared deviations (SS): for C2 - $SS=1139.06$, C19 - $SS=745.29$, C32 - $SS=743.32$. For other indicators, the contribution of the factors is statistically insignificant.

Univariate Tests of Significance for C0 (SpreadsheetBerezhna_fact Sigma-restricted parameterization Effective hypothesis decomposition)					
Effect	SS	Degr. of Freedom	MS	F	p
Intercept		0			
"C1"	56,336	1	56,336	0,37694	0,54310
"C2"	1139,06	1	1139,06	7,62153	0,00901
"C3"		0			
"C4"		0			
"C5"	214,44	1	214,44	1,43486	0,23880
"C6"	71,47	1	71,47	0,47826	0,49364
"C7"	491,99	1	491,99	3,29195	0,07796
"C8"	490,03	1	490,03	3,27886	0,07853
"C9"	0,24	1	0,24	0,00162	0,96804
"C10"	1,89	1	1,89	0,01266	0,91101
"C11"	87,53	1	87,53	0,58570	0,44907
"C12"	92,54	1	92,54	0,61924	0,43648
"C13"	63,79	1	63,79	0,42684	0,51769
"C14"	17,60	1	17,60	0,11780	0,73342
"C15"	258,23	1	258,23	1,72785	0,19699
"C16"	525,04	1	525,04	3,51308	0,06901
"C17"	34,89	1	34,89	0,23348	0,63187
"C18"	532,79	1	532,79	3,56496	0,06709
"C19"	745,29	1	745,29	4,98677	0,03184
"C20"	108,76	1	108,76	0,72777	0,39924
"C21"	198,04	1	198,04	1,32510	0,25726
"C22"	76,57	1	76,57	0,51235	0,47873
"C23"	377,21	1	377,21	2,52393	0,12087
"C24"	57,48	1	57,48	0,38460	0,53905
"C25"	220,96	1	220,96	1,47850	0,23192
"C26"	87,72	1	87,72	0,58695	0,44859
"C27"	217,14	1	217,14	1,45290	0,23592
"C28"	30,97	1	30,97	0,20723	0,65167
"C29"	270,96	1	270,96	1,81304	0,18656
"C30"	2,95	1	2,95	0,01974	0,88904
"C31"	212,79	1	212,79	1,42382	0,24057
"C32"	743,32	1	743,32	4,97360	0,03206
Error	5380,33	36	149,45		

Figure 2.9 – Univariate Tests of Significance of the influence of the state factors of combating financial cyber fraud on the level of cyber security for the countries of the world

The second step of the third stage (also confirmation of the statistical significance of 3 indicators that determine the state of combating financial cyber fraud, which affect the level of cyber security) is the construction of a Pareto Chart of t-Values of the significance of the influence of factors that determine the state of combating financial cyber fraud on the level of cyber security (Figure 2.10). The Pareto chart clearly helps to graphically visualize 80% of influential factors and 20% of non-influential factors.

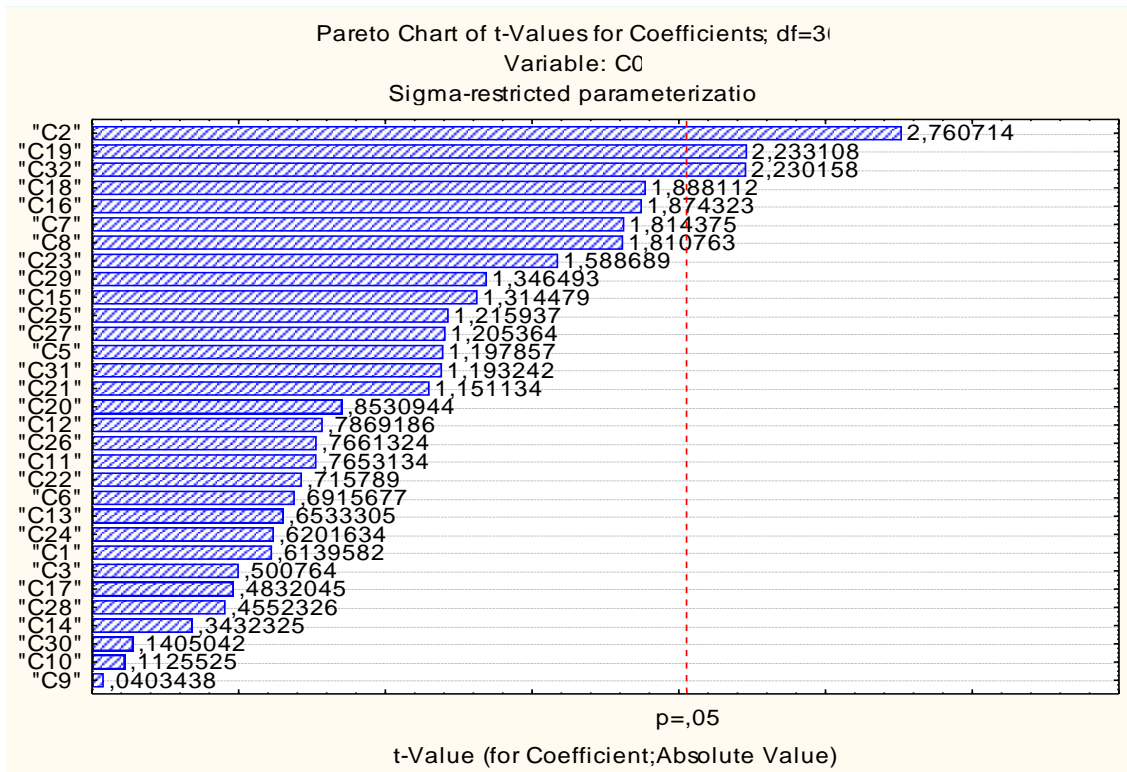


Figure 2.10 – Pareto Chart of t-Values of the significance of the influence of factors determining the state of combating financial cyber fraud on the level of cyber security for the countries of the world

Figure 2.10 shows 3 bands of indicators C2, C19, C32 crossing the red line (the limit of the critical permissible level of the Fisher test (p) 0.05 and means their statistical significance. That is, indicators C2, C19, C32 exert 80% influence, therefore there is relevant factors determining the state of anti-financial cyber fraud, which are proposed to be used in further research. Additionally, the Pareto Chart helps to rank the indicators from the most influential to the least influential indicator.

The third step of stage 3 is the correlation analysis. A correlation matrix of interdependence of relevant factors determining the state of combating financial cyber fraud and the level of cyber security was constructed (Figure 2.11).

of Significance , the construction of a Pareto Chart of t-Values of the significance of the influence of factors, the construction of a correlation matrix of interdependence of relevant factors, the most influential factors were established: C1, C2, C5, C23; C3, C4, C6, C9, C10, C20, C21, C22, C24, C25, C26, C27.

Similarly, for the cluster of 7 countries with Ukraine, a correlation matrix of interdependence of relevant factors determining the state of combating financial cyber fraud and the impact on the level of cyber security was constructed (Figure 2.12).

Correlations (SpreadsheetBerezhna_fact_c13.sta)															
Marked correlations are significant at $p < ,05000$															
N=7 (Casewise deletion of missing data)															
Variable	Means	Std.Dev.	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
C0	66	17	1,00000	0,78822	-0,23644	-0,19299	-0,19299	0,86492	0,44080	0,59947	-0,46451	0,68914	-0,73231	0,06086	0,183
C1	58	12	0,78822	1,00000	-0,50362	0,06660	0,06660	0,97538	0,65236	0,92573	-0,77797	0,85177	-0,67752	0,30235	0,521
C2	5	1	-0,23644	-0,50362	1,00000	0,29499	0,29499	-0,43960	-0,72795	-0,66914	0,66109	-0,27507	-0,06098	-0,52887	-0,538
C3	81	11	-0,19299	0,06660	0,29499	1,00000	1,00000	0,11718	-0,24424	0,05659	-0,26578	0,35008	-0,35784	0,12249	-0,308
C4	81	11	-0,19299	0,06660	0,29499	1,00000	1,00000	0,11718	-0,24424	0,05659	-0,26578	0,35008	-0,35784	0,12249	-0,308
C5	1	0	0,86492	0,97538	-0,43960	0,11718	0,11718	1,00000	0,56939	0,85638	-0,78372	0,88537	-0,75844	0,28537	0,403
C6	1	0	0,44080	0,65236	-0,72795	-0,24424	-0,24424	0,56939	1,00000	0,72372	-0,36970	0,22114	-0,02776	0,66416	0,491
C7	75807	99126	0,59947	0,92573	-0,66914	0,05659	0,05659	0,85638	0,72372	1,00000	-0,79408	0,78618	-0,56996	0,26611	0,459
C8	9	3	-0,46451	-0,77797	0,66109	-0,26578	-0,26578	-0,78372	-0,36970	-0,79408	1,00000	-0,84211	0,54996	-0,30345	-0,450
C9	1	1	0,68914	0,85177	-0,27507	0,35008	0,35008	0,88537	0,22114	0,78618	-0,84211	1,00000	-0,90175	-0,03914	0,199
C10	43	22	-0,73231	-0,67752	-0,06098	-0,35784	-0,35784	-0,75844	-0,02776	-0,56996	0,54996	-0,90175	1,00000	0,29697	0,159
C11	32	16	0,06086	0,30235	-0,52887	0,12249	0,12249	0,28537	0,66416	0,26611	-0,30345	-0,03914	0,29697	1,00000	0,495
C12	11	13	0,18383	0,52191	-0,53862	-0,30823	-0,30823	0,40301	0,49183	0,45910	-0,45084	0,19917	0,15973	0,49540	1,000
C13	3	3	-0,58546	-0,51325	-0,16462	-0,03181	-0,03181	-0,57108	0,12481	-0,19427	0,37827	-0,55304	0,50854	0,03090	-0,453
C14	27	23	0,20542	0,48715	-0,49300	-0,21054	-0,21054	0,41188	0,46968	0,36193	-0,44411	0,16575	0,18169	0,64878	0,961
C15	11	10	0,38172	0,57385	-0,55051	-0,53113	-0,53113	0,45944	0,69152	0,50300	-0,29446	0,13196	0,13431	0,48769	0,915
C16	13	8	-0,36276	-0,48695	0,46176	-0,05899	-0,05899	-0,53296	0,05625	-0,43988	0,84186	-0,68486	0,44366	0,00843	-0,393
C17	30	19	-0,22658	-0,15172	-0,46921	0,01092	0,01092	-0,12633	0,39811	-0,11144	-0,05090	-0,38462	0,56709	0,84561	0,163
C18	1	1	-0,39579	-0,31705	0,69970	0,65581	0,65581	-0,29799	-0,33352	-0,44957	0,40769	-0,25870	0,13400	0,15559	-0,226
C19	875453	206761	-0,39900	-0,40344	0,75927	0,62250	0,62250	-0,36713	-0,77381	-0,38457	0,27017	0,03010	-0,25706	-0,64826	-0,635
C20	78	10	0,89882	0,85877	-0,07281	0,11638	0,11638	0,91402	0,31658	0,62362	-0,55708	0,81997	-0,81448	0,08790	0,303

Figure 2.12 – Correlation matrix of interdependence of relevant factors that determine the state of combating financial cyber fraud and the level of cyber security for the cluster of 7 countries with Ukraine

Figure 2.12 shows that the calculated correlation coefficients between the resulting indicator C0 and the factor indicators have the following relationship: a strong relationship - the correlation coefficient between C0 and C1 is equal to 0.78, C5 – 0.86, C20 – 0, 89, C22 – 0.93, C23 – 0.77. Thus, the most influential factors were determined for the cluster of 7 countries with Ukraine: C1, C5, C20, C22, C23.

Stage 4 – determining the strength and direction of influence of relevant factors that determine the state of combating financial cyber fraud on the level of cyber security; construction of multiple linear regression using the method of least squares (OLS method).

The first step of the 4th stage is to determine the strength of the influence, as well as the direction of the influence of the relevant factors identified for the countries of the world, which determine the state of combating financial cyber fraud, on the level of cyber security, for the construction of a multiple linear regression. To build a multiple linear regression, we first use all 32 factors that determine the state of combating financial cyber fraud, affect the effective factor C0 (cyber security level). Figure 2.13 shows the estimated indicators of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud.

Figure 2.13 shows that not all factors determining the state of combating financial cyber fraud are statistically significant. That is, statically significant factors are: C1, C2, C16, C8, C6. Which was also partially determined in the second stage of the study. Since the built model is not sufficiently adequate according to the calculated indicators of the regression analysis, it is not advisable to build a model of linear multiple regression dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud based on these data.

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna R= ,90561669 R?= ,82014159 Adjusted R?= ,78089975 F(12,55)=20,900 p<,00000 Std.Error of estimate: 11,139						
N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(55)	p-level
Intercept			39,23211	23,1807	1,69241	0,096211
C1	0,599391	0,127161	0,87771	0,18621	4,71361	0,000011
C2	-0,395631	0,110911	-8,20131	2,29921	-3,56681	0,000751
C16	0,235391	0,079421	0,26931	0,09091	2,96351	0,004481
C15	-0,117171	0,070391	-0,24591	0,14771	-1,66441	0,101711
C8	0,188831	0,062221	1,85731	0,61191	3,03481	0,003671
C6	0,190871	0,080131	20,19921	8,48011	2,38191	0,020701
C11	-0,065241	0,067961	-0,10751	0,11201	-0,96001	0,341241
C29	-0,107261	0,073761	-0,09901	0,06811	-1,45411	0,151591
C22	-0,096471	0,077871	-0,10631	0,08581	-1,23891	0,220641
C18	0,113981	0,082451	0,42611	0,30821	1,38231	0,172441
C7	0,072721	0,063471	0,00001	0,00001	1,14561	0,256911
C12	-0,079041	0,073301	-0,16981	0,15751	-1,07821	0,285631

Figure 2.13 – Estimated indicators of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud of the countries of the world (32 indicators)

Therefore, a similar regression analysis was performed again, but for the dependence between the level of cyber security and 5 relevant factors (Figure 2.14), the estimated indicators of the regression analysis of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud are displayed.

Regression Summary for Dependent Variable: C0 (SpreadsheetBere)						
R= ,87543336 R ² = ,76638357 Adjusted R ² = ,74754354 F(5,62)=40,678 p<,00000 Std.Error of estimate: 11,957						
N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(62)	p-level
Intercept			24,8909	22,2257	1,1199	0,26707
C1	0,60722	0,10276	0,8891	0,1504	5,9091	0,00000
C2	-0,38336	0,11043	-7,9469	2,2893	-3,4713	0,00094
C6	0,09833	0,07894	10,4056	8,3542	1,2455	0,21761
C8	0,16519	0,06406	1,6248	0,6301	2,5786	0,01230
C16	0,27409	0,07579	0,3136	0,0867	3,6162	0,00060

Figure 2.14 – Estimated indicators of the regression analysis of the dependence between the level of cyber security and 5 factors that determine the state of combating financial cyber fraud in the countries of the world (5 indicators)

The model is sufficiently adequate (described in section 2.1). Next, according to the indicators in Figure 2.14, we formulate a model of linear multiple regression dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud of the countries of the world (although one factor is not relevant):

$$C0 = 24,8909 + 0,8891 \cdot C1 - 7,9769 \cdot C2 + 10,4056 \cdot C6 + 1,6248 \cdot C8 + 0,3136 \cdot C16 \quad (2.1)$$

Next, since one factor is not relevant, another regression analysis was performed, but for the dependence between the level of cyber security and 4 relevant factors (Figure 2.15).

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna)						
R= ,87208824 R ² = ,76053789 Adjusted R ² = ,74533395						
F(4,63)=50,022 p<,00000 Std.Error of estimate: 12,009						
N=68	Beta	Std.Err. of Beta	B	Std.Err. of B	t(63)	p-level
Intercept			40,7909	18,2735	2,2322	0,02916
C1	0,60410	0,10317	0,8845	0,1510	5,8549	0,00000
C2	-0,44057	0,10086	-9,1329	2,0909	-4,3677	0,00004
C8	0,14274	0,06174	1,4040	0,6073	2,3118	0,02406
C16	0,26851	0,07599	0,3073	0,0869	3,5334	0,00077

Figure 2.15 – Estimated indicators of the regression analysis of the dependence between the level of cyber security and 4 relevant factors that determine the state of combating financial cyber fraud of the countries of the world (4 indicators)

According to the indicators in Figure 2.15, we formulate a model of linear multiple regression dependence between the level of cyber security and 4 relevant factors that determine the state of combating financial cyber fraud in the countries of the world:

$$C0 = 40.7909 + 0,8845 \cdot C1 - 9,1329 \cdot C2 + 1,4040 \cdot C8 + 0,3073 \cdot C16 \quad (2.2)$$

The resulting model is adequate and accurate, which is described in point 2.1 for stage 4. All factors selected for the model are statistically significant, as evidenced by Student's tests and p-levels (which are not higher than the permissible critical level of 0.05). The following analysis of the indicators of the model of linear multiple regression dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for the countries of the world (2) allows us to formulate the following conclusions:

– indicator of C1, C8, C16 is the stimulator of the level of cyber security (an increase in this factor causes growth as a productive factor of the level of cyber security); so an increase in C1 by 1 unit causes an increase in the level of cyber security by 0.8845 units; an increase in C8 by 1 unit causes an increase in the level of cyber security by 1.4040 units; an increase in C16 by 1 unit causes an increase in the level of cyber security by 0.3073 units;

– the disincentive of the level of cyber security is the C2 indicator (an increase in this factor causes a decrease in both the effective factor of the level of cyber security), so an increase in C2 by 1 unit causes a decrease in the level of cyber security by 9.1329 units;

– other factors do not have a statistically significant impact on the level of cyber security.

The second step of the 4th stage is to determine the strength of influence, as well as the direction of influence of the relevant factors identified for the countries of the cluster with Ukraine, which determine the state of combating financial cyber fraud, on the level of cyber security, for the construction of a multiple linear regression. Actions are carried out similar to the previous regression analysis for 68 countries of the world. The forces of influence, as well as the directions of influence of relevant factors identified for the cluster of 7 countries with Ukraine, were determined, and a multiple linear regression was constructed using the method of least squares (OLS-method).

To build a multiple linear regression, we first use all 32 factors that determine the state of combating financial cyber fraud, affect the level of cyber security and the effective factor C0. Figure 2.16 shows the calculated indicators of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud. Where we observe the absence of dependencies with such a set of factors.

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezh)						
R=1,00000000 R ² =1,00000000 Adjusted R ² =1,00000000						
F(6,0)= -- p< -- Std.Error of estimate: ----						
N=7	Beta	Std.Err. of Beta	B	Std.Err. of B	t(0)	p-level
Intercept			65,6617			
C22	-0,88938		-6,8916			
C21	0,21539		0,0751			
C6	0,25813		17,3563			
C27	0,17988		3,3472			
C10	-0,08203		-0,0654			
C25	0,00387		0,1312			

Figure 2.16 – Estimated indicators of the regression analysis of the dependence between the level of cyber security and the factors determining the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (32 indicators)

Therefore, for a certain cluster of countries, a regression analysis was performed again, but for the dependence between the level of cyber security and the factors that determine the state of anti-financial cyber fraud (which was determined during the correlation analysis). Figure 2.17 shows the estimated indicators of the regression analysis of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud.

According to the obtained data of Figure 2.17, we can see that the factors are not statistically significant, but the dependence exists.

Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fac R= ,99327194 R?= ,98658915 Adjusted R?= ,91953493 F(5,1)=14,713 p<,19528 Std.Error of estimate: 4,9050						
N=7	Beta	Std.Err. of Beta	B	Std.Err. of B	t(1)	p-level
Intercept			12,7802	67,3081	0,1898	0,88054
C1	1,50058	1,30593	2,1251	1,8492	1,1490	0,45591
C5	-0,24016	0,96682	-49,3960	198,856	-0,2484	0,84500
C20	0,16138	0,39096	0,2750	0,6663	0,4127	0,75078
C22	-0,83656	0,25895	-6,4823	2,0066	-3,2304	0,19111
C23	-1,1829	0,77054	-1,6556	1,0782	-1,5351	0,36755

Figure 2.17 – Estimated indicators of the regression analysis of the dependence between the level of cyber security and the factors determining the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (5 indicators)

Next, according to the indicators in Figure 2.17, we formulate a model of linear multiple regression dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud:

$$C0 = 12,7802 + 2,1251 \cdot C1 - 49,3960 \cdot C5 + 0,2750 \cdot C20 - 6,4823 \cdot C22 - 1,6556 \cdot C23 \quad (2.3)$$

The following analysis of the indicators of the model of linear multiple regression dependence for the selected cluster with Ukraine between the level of

cyber security and relevant factors determining the state of combating financial cyber fraud (2.3) allows us to formulate the following conclusions:

– the stimulator of the level of cyber security is the indicator C1, C20 (increase in this factor causes growth as a productive factor of the level of cyber security); so an increase in C1 by 1 unit causes an increase in the level of cyber security by 2.1251 units; an increase in C20 by 1 unit causes an increase in the level of cyber security by 0.2750 units;

– indicators C5, C22, C23 are the demotivators of the level of cyber security (an increase in these factors causes a decrease in the effective factor of the level of cyber security), so an increase in C5 by 1 unit causes a decrease in the level of cyber security by 49.3960 units; an increase in C22 by 1 unit causes a decrease in the level of cyber security by 6.4823 units; an increase in C23 by 1 unit causes a decrease in the level of cyber security by 1.6556 units;

– other factors do not have a statistically significant impact on the level of cyber security.

2.3. Development of a software application for automating calculation methods

The automation of calculation methods in the work was performed with the help of MS Excel and the Statistica program.

Stage 1. Formation of the statistical base of the study - visualization of the input information base of the study in MS Excel (Figure 2.18) and in the Statistica program (Figure 2.19).

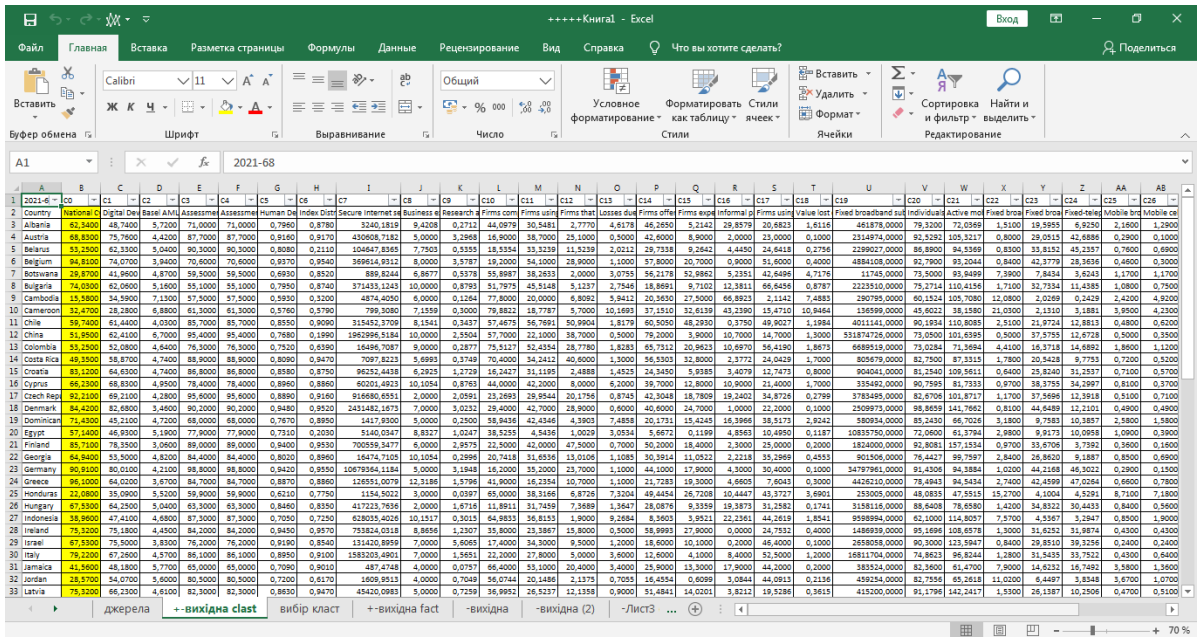


Figure 2.18 - Visualization of the input research information base in MS Excel

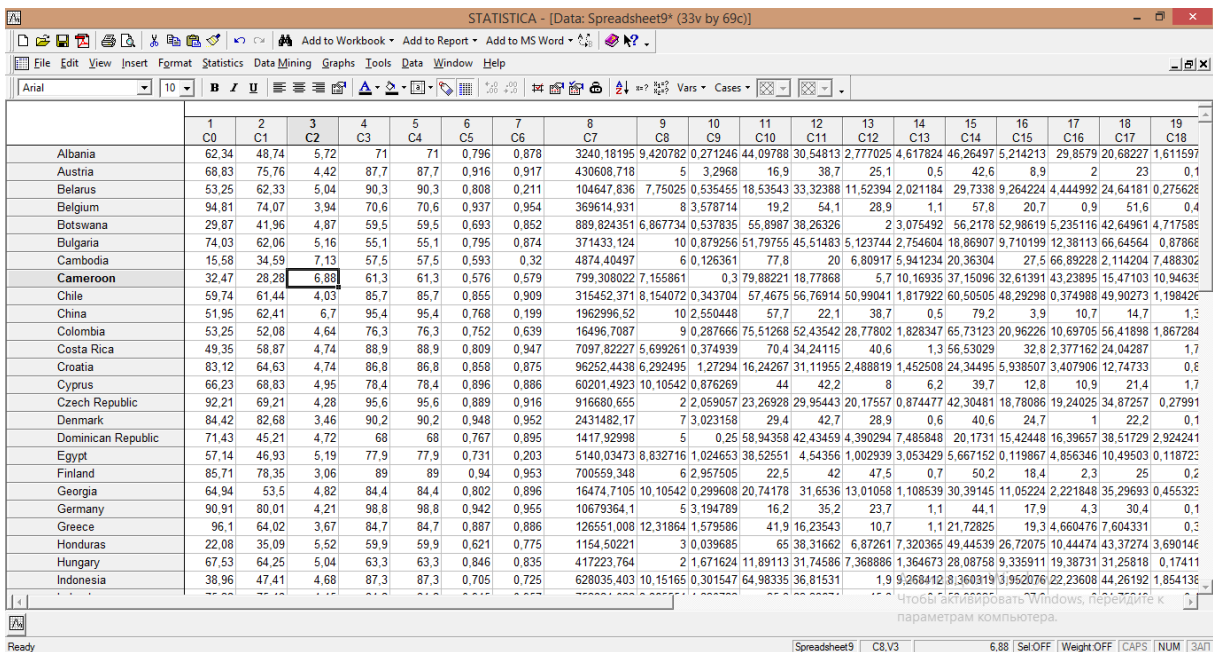


Figure 2.19 – Visualization of the input research information base of the Statistica program

Stage 2. Cluster analysis – implementation of cluster analysis in the Statistica program (Figure 2.20) and comparison of variance analysis indicators for cluster selection in MS Excel (Figure 2.21). The Statistica toolkit, the package "Multivariate

Exploratory Techniques" - "Canonical Analysis" - k-means clustering - analysis of variance - was used for dispersion analysis; "Multivariate Exploratory Techniques" - "Canonical Analysis" - k-means clustering— Member of each clusters – to directly distinguish certain groups of countries that are typical for their characteristics.

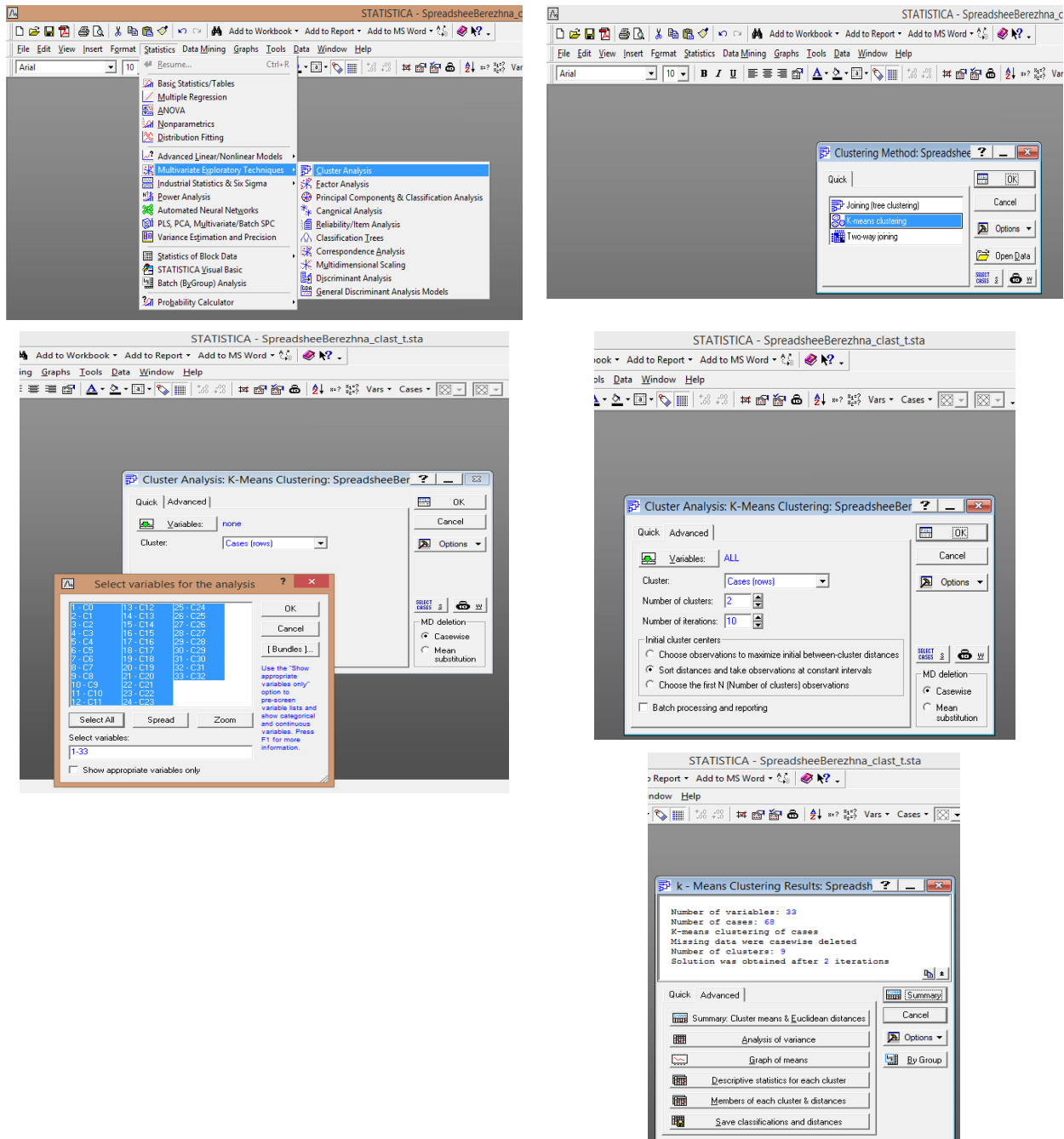


Figure 2.20 – Step-by-step implementation of cluster analysis in the Statistica program

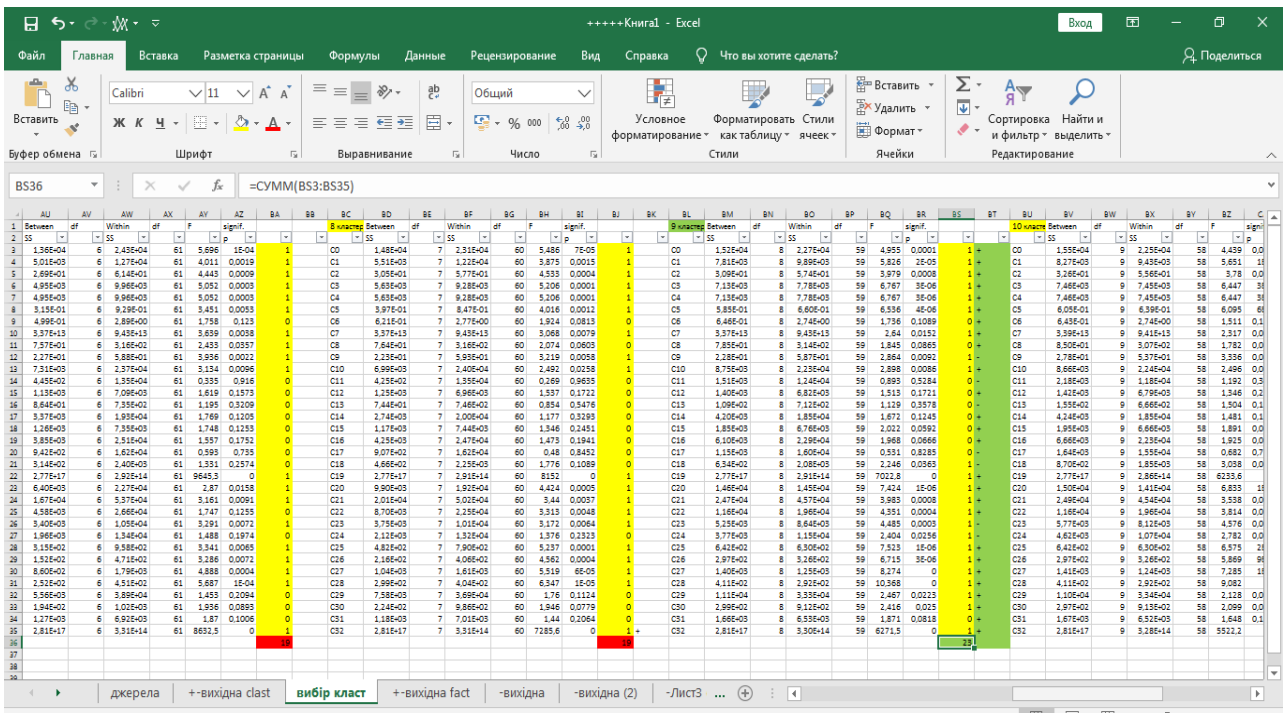


Figure 2.21 – The result of the comparison of variance analysis indicators for cluster selection in MS Excel

Formation of cluster analysis results in the Statistica program: formed clusters, average values of indicators within clusters, Euclidean distances between clusters (Figure 2.22, Figure 2.23).

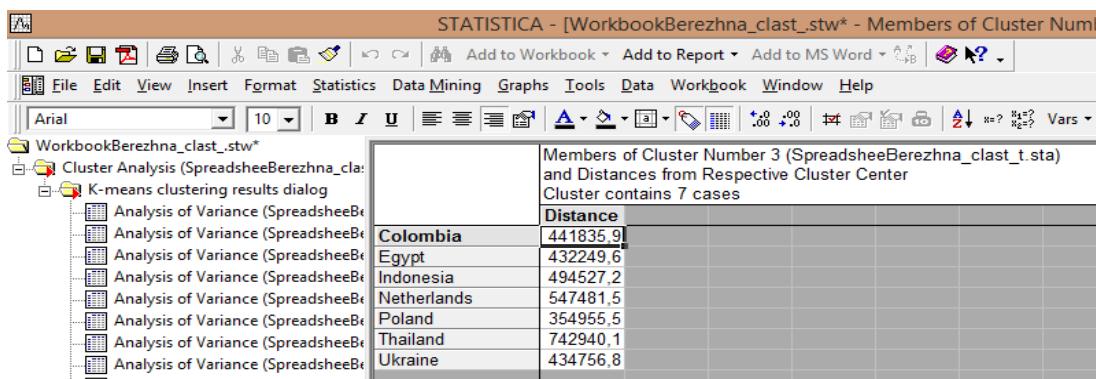


Figure 2.22 – Obtaining the results of cluster analysis in the Statistica program (formed clusters)

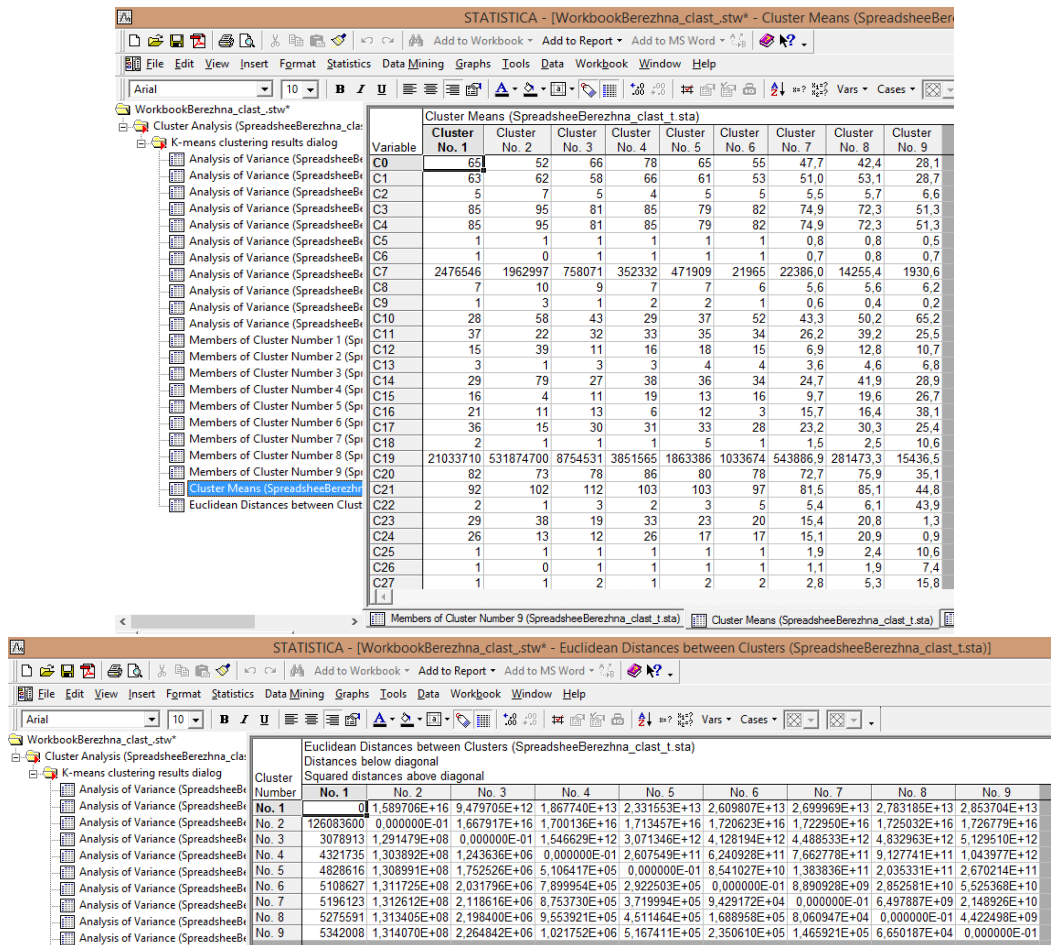


Figure 2.23 – Obtaining the results of cluster analysis in the Statistica program (average values of indicators within clusters, Euclidean distances between clusters)

Stage 3. Factor analysis – implementation of factor analysis in the Statistica program using methods of sigma-limited parameterization and correlation analysis (Figure 2.24). At this stage, the "Statistics" toolkit, the package "Advanced Linear/Nonlinear Models" General Regression Models" - "General linear models" are used.

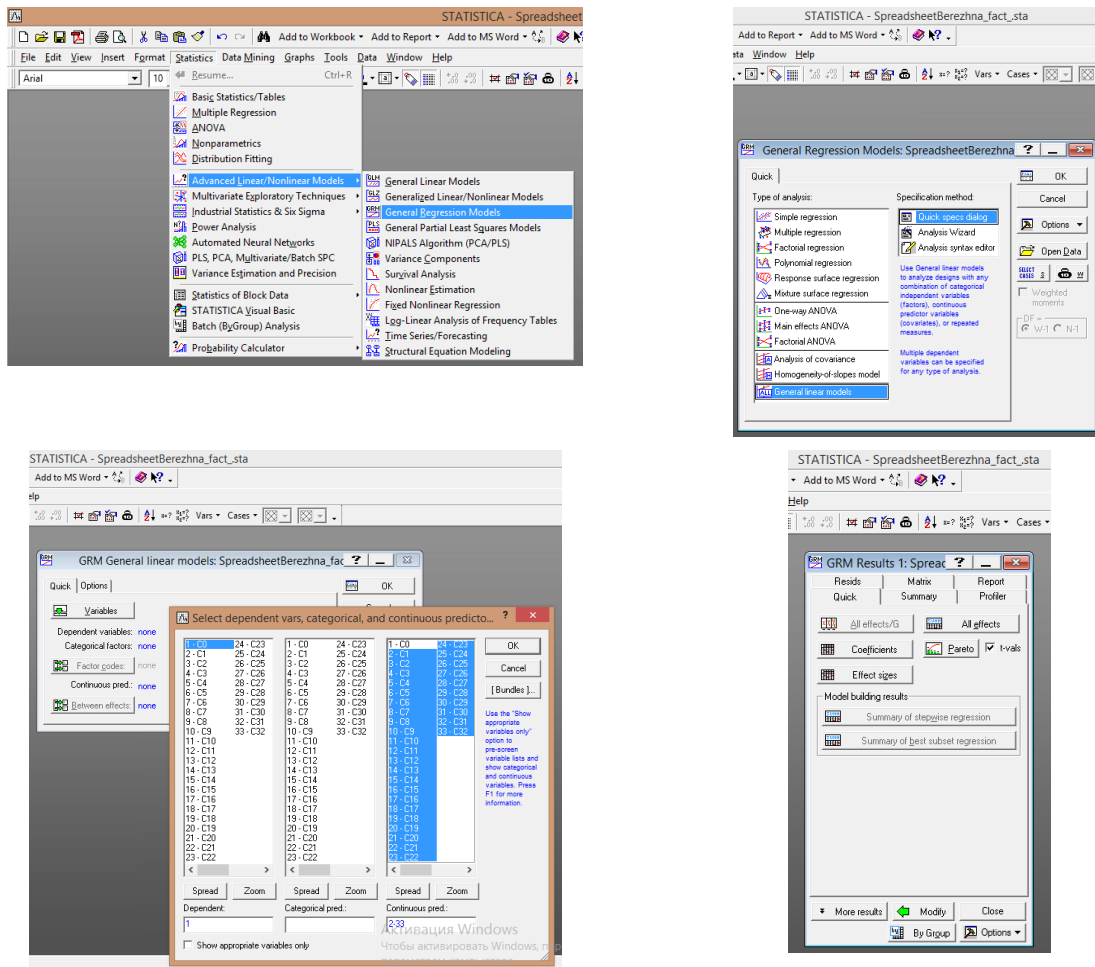


Figure 2.24 – Step-by-step implementation of factor analysis in the Statistica program

Formation of the results of factor analysis in the Statistica program: construction of Univariate Tests of Significance of the influence of factors and Pareto Chart of t-Values of the significance of the influence of factors (Figure 2.25).

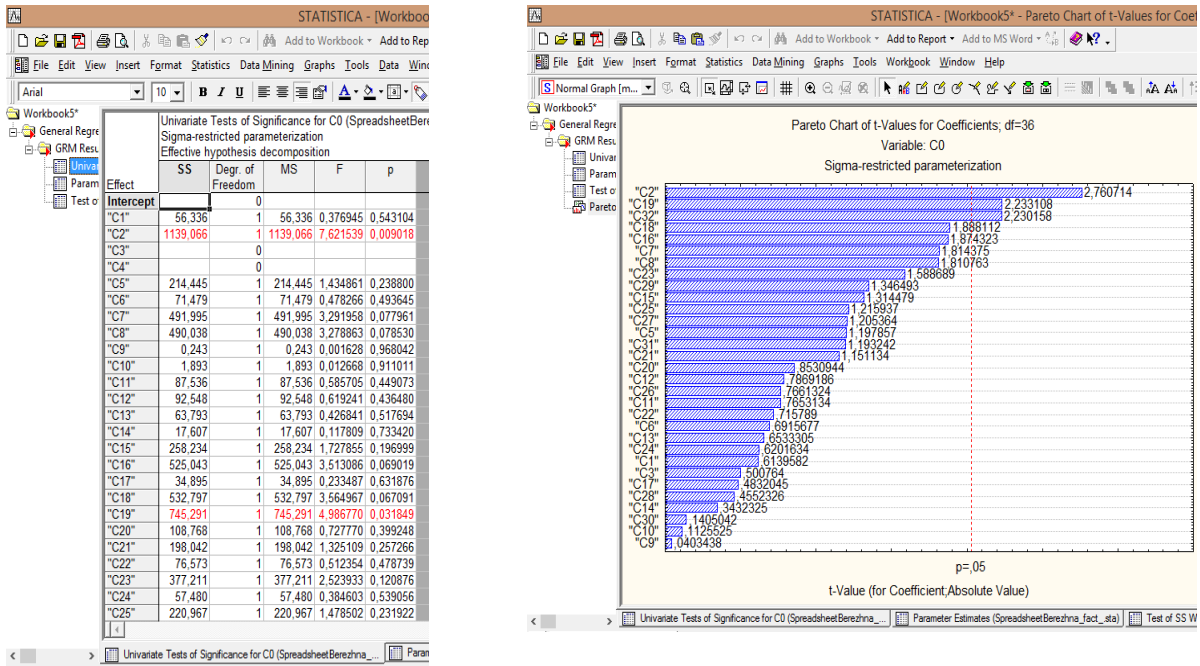


Figure 2.25 - Obtaining the results of factor analysis in the Statistica program (Univariate Tests of Significance and Pareto Chart of t-Values)

Performing a correlation analysis in the Statistica program (Figure 2.26) and presenting its results - a correlation matrix of interdependence of relevant factors (Figure 2.27). At this stage, the "Statistics" toolkit, the "Basic Statistics/Tables" - "Correlation matrices" package are used.

Stage 4. Determining the strength of influence and direction of influence of relevant factors; construction of multiple linear regression by the method of least squares - OLS method - implementation of regression analysis, obtaining results in the Statistica program (Figure 2.28) and presenting the adequacy of the model (Figure 2.29). At this stage, the "Statistics" toolkit, the "Multiple Regression" - "Consolidated Regression" package was used.

The figure illustrates the step-by-step implementation of regression analysis in the Statistica program. It consists of four screenshots:

- Screenshot 1:** The "Statistics" menu is open, showing the "Multiple Regression" option selected.
- Screenshot 2:** The "Multiple Linear Regression: Spreadsheet" dialog box is shown. The "Dependent" variable is set to "none" and the "Independent" variable is set to "none". A "Select dependent and independent variable lists" dialog box is also visible, showing the selection of variables C0 through C12.
- Screenshot 3:** The "Multiple Regression Results: SpreadsheetBerezhna_fact_sta" dialog box is shown. It displays the following regression results:

Parameter	Value
Multiple R	.90561669
F	20.89968
R ²	.82014159
df	12.55
adjusted R ²	.78089975
p	.000000
Standard error of estimate	11.138843541
Intercept	35.232158798
Std. Error	23.18071
t (55)	1.6924
p	.0962

 The regression coefficients (betas) are also listed:

Variable	Beta
C1	.589
C2	.40
C3	.288
C4	.12
C5	.189
C6	.191
C7	.07
C8	.11
C9	.10
C10	.114
C11	.073
C12	.08
- Screenshot 4:** The "Regression Summary for Dependent Variable: C0 (SpreadsheetBerezhna_fact_sta)" dialog box is shown. It displays the following regression summary:

Parameter	Beta	Std. Err. of Beta	B	Std. Err. of B	t (55)	p-level
Intercept			39.23216	23.18071	1.69245	0.096219
C1	0.599399	0.127163	0.87770	0.18621	4.71363	0.000017
C2	-0.395630	0.110917	-8.20131	2.29929	-3.56689	0.000757
C3	0.235390	0.079429	0.28939	0.09090	2.96355	0.004487
C4	-0.117170	0.070397	-0.24592	0.14775	-1.66441	0.101719
C5	0.188830	0.062220	1.85732	0.61199	3.03487	0.003671
C6	0.190875	0.080134	20.19924	8.48016	2.38194	0.020708
C7	-0.065245	0.067962	-0.10758	0.11206	-0.96002	0.341245
C8	-0.107269	0.073769	-0.09908	0.06814	-1.45413	0.151592
C9	-0.096476	0.077872	-0.10636	0.08585	-1.23890	0.220642
C10	0.113988	0.082458	0.42612	0.30825	1.38237	0.172445
C11	0.072721	0.063477	0.00000	0.00000	1.14563	0.256911
C12	-0.079040	0.073304	-0.16987	0.15755	-1.07825	0.286631

Figure 2.28 – Step-by-step implementation of regression analysis in the Statistica program

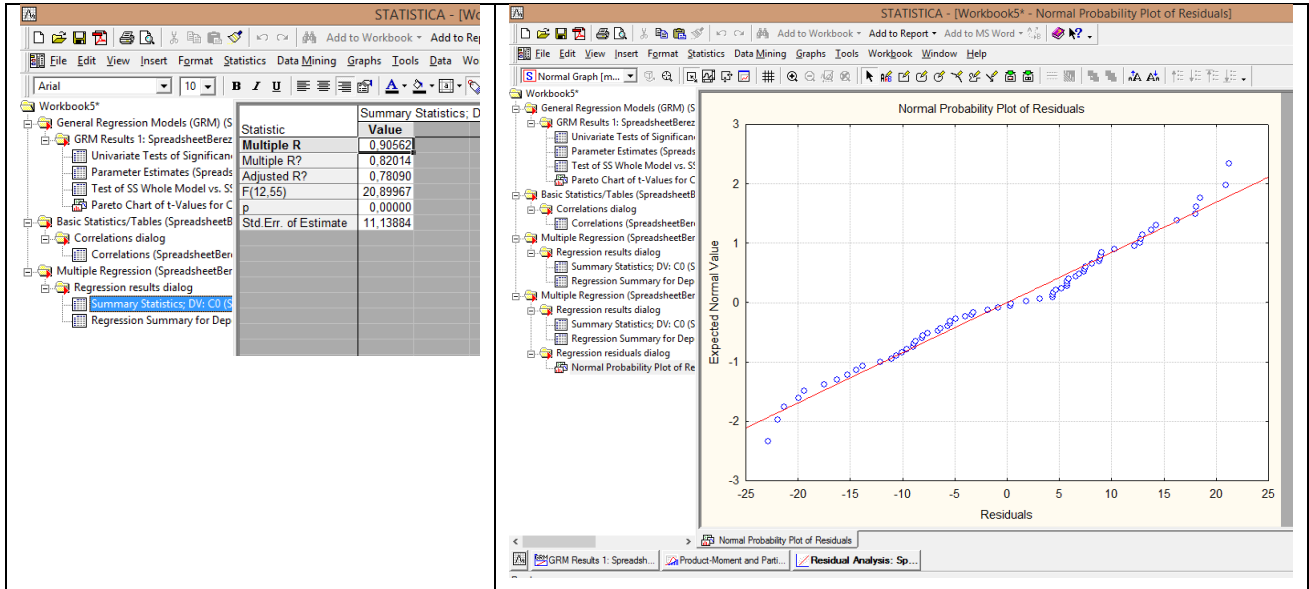


Figure 2.29 – Visualization of the adequacy of the regression analysis model in the Statistica program (indicators of the adequacy of the regression analysis and a graphical representation of compliance with the normal distribution law)

CONCLUSIONS

The analysis of the results of global and domestic research allows to identify and evaluate priorities and trends in the modern financial market, shifting the vector of research in the direction of studying the problems of cybercrime.

In the work, the interpretation of the concept of due diligence was formed, its normative basis was outlined, a number of stages and features were developed regarding the implementation of due diligence of enterprises in the aspect of combating financial cyber fraud, a structural and logical diagram of the stages and features of the implementation of due diligence of enterprises was built.

In the course of the study, modern methods of due diligence modeling were highlighted: a due diligence model based on machine learning, a due diligence model based on risk assessment; due diligence models based on deep learning of NLP; NAP, mHRDD, BHR models of the optimality of the assessment of the implementation of the UN guidelines on business and human rights, a model of consensus multidimensional verification of investment projects based on financial technologies, a computer model of due diligence through AHP and big data. Also, the paper highlights the modeling approaches of countering financial cyber fraud: a model of the image of a cybercrime victim; an econometric model of the impact of digitalization on economic transformations based on developed quantile regressions (taking into account the national cyber security indicator); machine learning model (SVM) to protect the financial sector from cybercrime; assessment models for assessing the influencing factors of cyber security awareness; a model of cybersecurity awareness for seniors.

The advantages of the implementation of the complex Due Diligence methodology in the aspect of countering financial cyber fraud for enterprises have been determined.

We completed the formulation of the modeling task and formulated the requirements for the model.

We developed a mathematical model that is implemented in 4 stages: we collected a statistical research base; performed a cluster analysis - grouping the countries of the world into clusters using the k-means method; conducted a factor analysis – determined the relevant factors characterizing the state of combating financial cyber fraud for the countries of the world, using the methods of sigma-limited parameterization and correlation analysis, conducted univariate tests of the significance of factors, constructed a Pareto diagram; implemented a regression analysis of the dependence between the factors that determine the state of combating financial cyber fraud, constructed multiple linear regressions.

Thus, the use of due diligence methods and models at enterprises will allow the formation of guiding principles and policies of financial security of enterprises, which in turn will help reduce the level of negative consequences, including financial cyber threats, financial cyber risks that may be present in business processes; to maximize possible positive effects from the adoption of management decisions formed taking into account a number of factors.

REFERENCES

1. Aman, A., & Reji, D. J. Environmental due diligence data: A novel corpus for training environmental domain NLP models. 2022. *Data in Brief*, 45 doi:10.1016/j.dib.2022.108579 (Last accessed: 01.03.2023).
2. Attiany, M. S., Al-Kharabsheh, S. A., Al-Makhariz, L. S., Abed-Qader, M. A., Al-Hawary, S. I. S., Mohammad, A. A., & Rahamneh, A. A. A. L. Barriers to adopt industry 4.0 in supply chains using interpretive structural modeling. 2023. *Uncertain Supply Chain Management*, 11(1), 299-306. doi:10.5267/j.uscm.2022.9.013 (Last accessed: 03.03.2023)
3. Bello, M., & Griffiths, M. Routine activity theory and cybercrime investigation in nigeria: How capable are law enforcement agencies? (2020) *Rethinking cybercrime: Critical debates* (pp. 213-235). 2023. doi:10.1007/978-3-030-55841-3_11 Retrieved from www.scopus.com (Last accessed: 03.03.2023)
4. Botchway, S., Tsiachristas, A., Pollard, J., & Fazel, S. Cost-effectiveness of implementing a suicide prediction tool (OxMIS) in severe mental illness: Economic modeling study. *European Psychiatry*, 66(1) doi:10.1192/j.eurpsy.2022.2354 (Last accessed: 03.03.2023)
5. Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. Development of organization, social and individual cyber security awareness model (osicsam) for the elderly. 2021 . *International Journal of Advanced Technology and Engineering Exploration*, 8(76), 511-519. doi:10.19101/IJATEE.2020.762185 (Last accessed: 07.03.2023)
6. Camoletto, S., Corazza, L., Pizzi, S., & Santini, E. Corporate social responsibility due diligence among european companies: The results of an interventionist research project with accountability and political implications.

2022. *Corporate Social Responsibility and Environmental Management*, 29(5), 1122-1133. doi:10.1002/csr.2258 (Last accessed: 07.03.2023)

7. Carannante, M., D'Amato, V., Fersini, P., Forte, S., & Melisi, G. Machine learning due diligence evaluation to increase NPLs profitability transactions on secondary market. 2023. *Review of Managerial Science*, doi:10.1007/s11846-023-00635-y (Last accessed: 07.03.2023)

8. Chitimira, H., & Munedzi, S. An evaluation of customer due diligence and related anti-money laundering measures in the united kingdom. 2023 . *Journal of Money Laundering Control*, 26(7), 127-137. doi:10.1108/JMLC-01-2023-0004 (Last accessed: 10.03.2023)

9. Dadhich, M., Hiran, K. K., Rao, S. S., Sharma, R., & Meena, R. *Study of combating technology induced fraud assault (TIFA) and possible solutions. 2022: The way forward* doi:10.1007/978-3-031-07012-9_59 Retrieved from www.scopus.com (Last accessed: 17.03.2023)

10. Deva, S. Mandatory human rights due diligence laws in europe: A mirage for rightsholders? 2023. *Leiden Journal of International Law*, doi:10.1017/S0922156522000802 (Last accessed: 17.03.2023)

11. Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups. 2014. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0095>. (Last accessed: 07.03.2023)

12. Elbel, J., Bose O'Reilly, S., & Hrzic, R. A european union corporate due diligence act for whom? 2023. Considerations about the impact of a european union due diligence act on artisanal and small-scale cobalt miners in the democratic republic of congo. *Resources Policy*, 81 doi:10.1016/j.resourpol.2022.103241 (Last accessed: 09.03.2023)

13. Guanipa, H. J., & Chimá, J. T Integrality human rights-rights of nature: Towards corporate due diligence and sustainable energy transition. [Integralidad

derechos humanos-derechos de la naturaleza: hacia la debida diligencia empresarial y la transición energética sostenible]. 2023. *Revista Derecho Del Estado*, (54), 307-344. doi:10.18601/01229893.n54.10 (Last accessed: 11.03.2023)

14. Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. Introduction of a corporate security risk management system: The experience of Poland. 2022. *Journal of Risk and Financial Management*, 15(8) doi:10.3390/jrfm15080335 (Last accessed: 07.03.2023)

15. Khan, M. R., Puneeth, V., Alqahtani, A. M., Alhazmi, S. E., Beinane, S. A. O., Shutaywi, M., Alsenani, T. R. Numerical simulation and mathematical modeling for heat and mass transfer in MHD stagnation point flow of nanofluid consisting of entropy generation. 2023. *Scientific Reports*, 13(1) doi:10.1038/s41598-023-33412-8 (Last accessed: 07.03.2023)

16. Kumagai, A., Jeong, S., Kim, D., Kong, H. -, Oh, S., & Lee, S. Validation of data mining models by comparing with conventional methods for dental age estimation in korean juveniles and young adults. 2023. *Scientific Reports*, 13(1) doi:10.1038/s41598-023-28086-1 (Last accessed: 11.03.2023)

17. Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. An approach to managing innovation to protect financial sector against cybercrime. 2021. [Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością] *Polish Journal of Management Studies*, 24(2), 276-291. doi:10.17512/pjms.2021.24.2.17 (Last accessed: 07.06.2023)

18. Kuzmenko, O., Šuleř, P., Lyeonov, S., Judrupa, I., & Boiko, A. Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions/ 2020. *Journal of International Studies*, 13(3), 332-339. doi:10.14254/2071-8330.2020/13-3/22 (Last accessed: 07.03.2023)

19. Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. Countering cybercrime risks in financial institutions: Forecasting information trends. 2022. *Journal of Risk and Financial Management*, 15(12) doi:10.3390/jrfm15120613 (Last accessed: 07.03.2023)

20. Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. 2022 . *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4) doi:10.3390/joitmc8040195 (Last accessed: 15.04.2023)

21. Lieonov, S., Hlawiczka, R., Boiko, A., Mynenko, S., & Garai-Fodor, M. Structural modelling for assessing the effectiveness of system for countering legalization of illicit money. 2022. *Journal of International Studies*, 15(3), 215-233. doi:10.14254/2071-8330.2022/15-3/15 (Last accessed: 15.03.2023)

22. Liesa, C. R. F. (2022). Business due diligence and human rights: Towards a spanish law. [La debida diligencia de las empresas y los Derechos Humanos: hacia una ley española] *Cuadernos De Derecho Transnacional*, 14(2), 427-455. doi:10.20318/cdt.2022.7190 (Last accessed: 07.03.2023)

23. Lin, K., & Gao, Y. Model interpretability of financial fraud detection by group SHAP. 2022. [formula presented]. *Expert Systems with Applications*, 210 doi:10.1016/j.eswa.2022.118354 (Last accessed: 16.03.2023)

24. Litwin, D. Business impacts on economic inequality: An agenda for defining related human rights impacts and economic inequality due diligence. 2023. *Business and Human Rights Journal*, 8(1), 90-96. doi:10.1017/bhj.2022.27 (Last accessed: 07.05.2023)

25. Liu, W., Sun, Y., Yüksel, S., & Dinçer, H. Consensus-based multidimensional due diligence of fintech-enhanced green energy investment projects/ 2021. *Financial Innovation*, 7(1) doi:10.1186/s40854-021-00289-3 (Last accessed: 19.03.2023)

26. Liu, Y., Feng, Y., & Zhou, B. Research on due diligence computer model of thermal power plant considering through AHP and big data. Paper presented at. 2021. *the Journal of Physics: Conference Series*, , 2033(1) doi:10.1088/1742-6596/2033/1/012061 Retrieved from www.scopus.com (Last accessed: 19.03.2023)

27. Li, Z. Operationalising the UN guiding principles on business and human rights through human rights due diligence: A critical assessment of current states practices. 2022. *Academic Journal of Interdisciplinary Studies*, 11(4), 8-21. doi:10.36941/ajis-2022-0094 (Last accessed: 17.04.2023)

28. Lu, T., Wang, C., Cao, Y., & Chen, H. Photovoltaic power prediction under insufficient historical data based on dendrite network and coupled information analysis. 2023. *Energy Reports*, 9, 1490-1500. doi:10.1016/j.egy.2022.12.076 (Last accessed: 17.05.2023)

29. Nicholls, J., Kuppa, A., & Le-Khac, N. – Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. 2021. *IEEE Access*, 9, 163965-163986. doi:10.1109/ACCESS.2021.3134076 (Last accessed: 07.05.2023)

29. Ren, D., Wang, C., Wei, X., Lai, Q., & Xu, W. Building a quantitative composition-microstructure-property relationship of dual-phase steels via multimodal data mining. 2023. *Acta Materialia*, 252 doi:10.1016/j.actamat.2023.118954 (Last accessed: 27.05.2023)

30. Roy, V., Desjardins, D., Fertel, C., & Ouellet-Plamondon, C. Methodology for conducting third-party risk-based due diligence in the construction and civil engineering industry. 2022. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 14(4) doi:10.1061/(ASCE)LA.1943-4170.0000553 (Last accessed: 07.05.2023)

31. Proposal for a directive of the european parliament and of the council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 23.02.2022. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071>. (Last accessed: 07.06.2023)

32. Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27. November 2019 on sustainability-related disclosures in the financial services sector. <https://eur-lex.europa.eu/legal->

[content/EN/TXT/?uri=CELEX%3A02019R2088-20200712](#). (Last accessed: 27.05.2023)

33. Sedano, T. G. Due diligence and criminal policy models in the fight against contemporary forms of slavery. [Diligencia debida y modelos de política criminal en la lucha contra las formas contemporáneas de esclavitud]. 2022. *Eunomia.Revista En Cultura De La Legalidad*, (22), 210-229. doi:10.20318/eunomia.2022.6813 (Last accessed: 17.05.2023)

34. Vasilyeva, T. A., Kuzmenko, O. V., Stoyanets, N. V., Artyukhov, A. E., & Bozhenko, V. V. The depiction of cybercrime victims using data mining techniques. 2022. [Побудова портрету кібержертви з використанням технологій data-mining] *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (5), 174-178. doi:10.33271/nvngu/2022-5/174 (Last accessed: 07.06.2023)

35. Vasilyeva, T., Ziółko, A., Kuzmenko, O., Kapinos, A., & Humenna, Y. Impact of digitalization and the covid-19 pandemic on the aml scenario: data mining analysis for good governance. 2021. *Economics and Sociology*, 14(4), 326-354. doi:10.14254/2071-789X.2021/14-4/19 (Last accessed: 07.03.2023)

36. Villiers, C. New directions in the european union's regulatory framework for corporate reporting, due diligence and accountability: The challenge of complexity . 2022. *European Journal of Risk Regulation*, 13(4), 548-566. doi:10.1017/err.2022.25 (Last accessed: 07.06.2023)

37. Wahid, S. D. M., Buja, A. G., Hasrol Jono, M. N. H., & Aziz, A. A. Assessing the influential factors of cybersecurity awareness in malaysia during the pandemic outbreak. 2021. A structural equation modeling. *International Journal of Advanced Technology and Engineering Exploration*, 8(74), 73-81. doi:10.19101/IJATEE.2020.S1762116 (Last accessed: 11.05.2023)

38. Zarrabeitia-Bilbao, E., Jaca-Madariaga, M., Rio-Belver, R. M., & Álvarez-Meaza, I. Nuclear energy: Twitter data mining for social listening analysis. 2023. *Social Network Analysis and Mining*, 13(1) doi:10.1007/s13278-023-01033-8 (Last accessed: 07.05.2023)

APPENDIXES

APPENDIX A

SUMMARY

Berezhna D. E. Economic and Mathematical Modeling of Due Diligence of Enterprises in the Combating Financial Cyber Frauds Aspect Based on Data Mining Methods. Bachelor's qualifying work. Sumy State University, Sumy, 2023.

The main goal of the work is to study and deepen the theoretical aspects of due diligence of enterprises in the aspect of countering financial cyber fraud, to determine the main factors and to develop a structural and logical model of due diligence of enterprises in the aspect of countering financial cyber fraud. The work describes the most important due diligence parameters of enterprises and aspects of combating financial cyber fraud; the current state of modeling of the researched issue is analyzed; an economic-mathematical model of due diligence of enterprises in the aspect of combating financial cyber fraud was developed; its adequacy was checked.

Keywords: due diligence, combating financial cyber fraud, level of cyber security, data mining, cluster analysis, k-means method, factor analysis, correlation analysis, regression analysis.

АНОТАЦІЯ

Бережна Д.Є. Економіко-математичне моделювання due diligence підприємств в аспекті протидії фінансовим кібершахрайствам на основі методів data mining. Кваліфікаційна робота бакалавра. Сумський державний університет, Суми, 2023 р.

Основною метою роботи є вивчення та поглиблення теоретичних аспектів Due diligence підприємств в аспекті протидії фінансовому кібершахрайству,

визначення основних факторів та розробка структурно-логічної моделі Due diligence підприємств в аспекті протидія фінансовому кібершахрайству. В роботі охарактеризоване найважливіші параметри Due diligence підприємств і аспекти протидії фінансовому кібершахрайству; проаналізовано поточний стан моделювання досліджуваного питання; розроблено економіко-математичну модель Due diligence підприємств в аспекті протидія фінансовому кібершахрайству; перевірено її адекватність.

Ключові слова: due diligence, протидії фінансовим кібершахрайствам, рівень кібербезпеки, data mining, кластерний аналіз, метод k-середніх, факторний аналіз, correlation analysis, regression analysis.

APPENDIX A.1

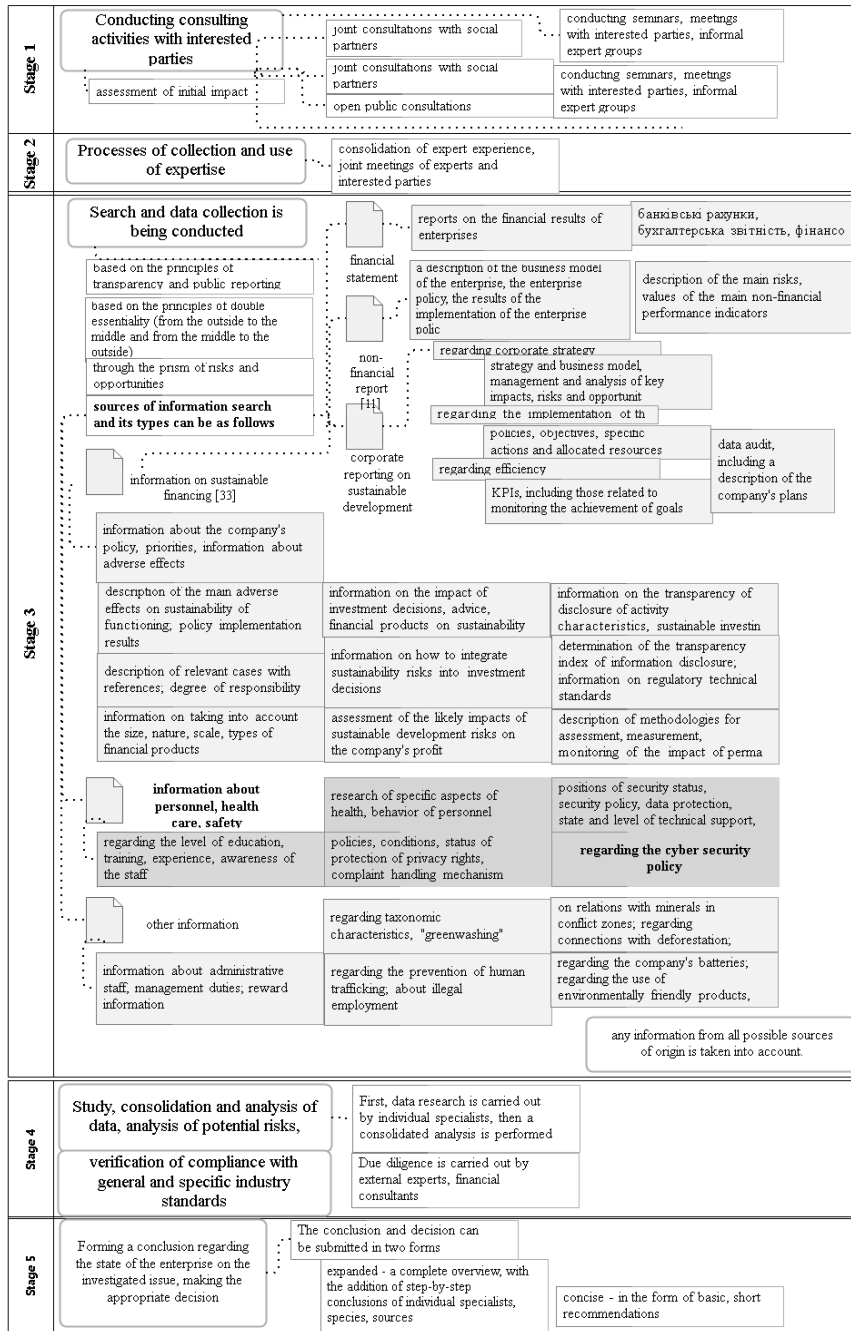


Figure A.1 – Structural and logical scheme of stages and features of due diligence implementation of enterprises

APPENDIX B

Variable	Analysis of Variance (SpreadsheetBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,584835E+0	1	3,792545E+0	66	0,028	0,86860
C1	5,867201E+0	1	1,763623E+0	66	0,220	0,64091
C2	2,173450E+0	1	8,611907E+0	66	1,666	0,20134
C3	3,721388E+0	1	1,453741E+0	66	1,690	0,19818
C4	3,721388E+0	1	1,453741E+0	66	1,690	0,19818
C5	3,766681E-0	1	1,244185E+0	66	0,000	0,98876
C6	3,096144E-0	1	3,078364E+0	66	6,638	0,01222
C7	2,265191E+1	1	1,257285E+1	66	1,189	0,27947
C8	9,809305E+0	1	3,823661E+0	66	1,693	0,19770
C9	2,434331E+0	1	7,906979E+0	66	2,032	0,15873
C10	2,043545E+0	1	3,081119E+0	66	0,438	0,51051
C11	1,215654E+0	1	1,383361E+0	66	0,580	0,44903
C12	6,208773E+0	1	7,593270E+0	66	5,397	0,02326
C13	1,160410E+0	1	8,092887E+0	66	0,946	0,33420
C14	2,060820E+0	1	2,064106E+0	66	6,589	0,01253
C15	1,584277E+0	1	8,454716E+0	66	1,237	0,27013
C16	2,391058E+0	1	2,894471E+0	66	0,059	0,81609
C17	2,282299E+0	1	1,687155E+0	66	0,893	0,34816
C18	4,029425E+0	1	2,710926E+0	66	0,098	0,75510
C19	2,746843E+1	1	2,664075E+1	66	6805,05	0,00000
C20	6,824450E-0	1	2,907542E+0	66	0,002	0,96872
C21	1,261738E+0	1	7,022190E+0	66	0,119	0,73166
C22	6,399877E+0	1	3,115048E+0	66	0,136	0,71387
C23	2,926449E+0	1	1,359611E+0	66	1,421	0,23757
C24	1,968024E+0	1	1,529383E+0	66	0,089	0,77163
C25	3,491276E+0	1	1,268697E+0	66	0,182	0,67136
C26	2,070302E+0	1	6,207251E+0	66	0,220	0,64048
C27	8,258200E+0	1	2,641704E+0	66	0,206	0,65115
C28	2,848000E+0	1	7,003815E+0	66	0,268	0,60615
C29	6,750698E+0	1	4,446805E+0	66	0,010	0,92057
C30	4,610975E+0	1	1,205540E+0	66	0,252	0,61703
C31	2,577170E+0	1	8,166954E+0	66	0,208	0,64962
C32	2,782984E+1	1	2,997111E+1	66	6128,46	0,00000

Variable	Analysis of Variance (SpreadsheetBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	2,689301E+0	2	3,767236E+0	65	0,23	0,79359
C1	2,218022E+0	2	1,747310E+0	65	0,41	0,66367
C2	2,238698E+0	2	8,605383E+0	65	0,85	0,43401
C3	1,456365E+0	2	1,345318E+0	65	3,52	0,03541
C4	1,456365E+0	2	1,345318E+0	65	3,52	0,03541
C5	1,549448E-0	2	1,228694E+0	65	0,41	0,66545
C6	5,380607E-0	2	2,849918E+0	65	6,14	0,00362
C7	1,971711E+1	2	1,082766E+1	65	5,92	0,00435
C8	2,864964E+0	2	3,635257E+0	65	2,56	0,08497
C9	2,933791E+0	2	7,857033E+0	65	1,21	0,30378
C10	1,317392E+0	2	2,969815E+0	65	1,44	0,24399
C11	1,275776E+0	2	1,382759E+0	65	0,30	0,74194
C12	7,376563E+0	2	7,476491E+0	65	3,21	0,04697
C13	1,546062E+0	2	8,054322E+0	65	0,62	0,53905
C14	3,356295E+0	2	1,934558E+0	65	5,64	0,00552
C15	4,610899E+0	2	8,152054E+0	65	1,84	0,16727
C16	1,185795E+0	2	2,885004E+0	65	0,13	0,87519
C17	2,746751E+0	2	1,682510E+0	65	0,53	0,59079
C18	3,162357E+0	2	2,683332E+0	65	0,38	0,68332
C19	2,766505E+1	2	6,979416E+1	65	12882,3	0,00000
C20	2,714414E+0	2	2,880466E+0	65	0,31	0,73724
C21	2,422327E+0	2	7,010584E+0	65	0,11	0,89395
C22	4,022389E+0	2	3,081224E+0	65	0,42	0,65604
C23	3,439870E+0	2	1,354477E+0	65	0,83	0,44260
C24	8,882727E+0	2	1,522468E+0	65	0,19	0,82773
C25	3,059474E+0	2	1,241594E+0	65	0,80	0,45332
C26	1,206867E+0	2	6,107267E+0	65	0,64	0,52941
C27	6,940018E+0	2	2,580562E+0	65	0,87	0,42211
C28	2,075418E+0	2	6,824753E+0	65	0,99	0,37772
C29	2,786284E+0	2	4,419617E+0	65	0,20	0,81526
C30	2,600176E+0	2	1,184149E+0	65	0,71	0,49365
C31	1,657930E+0	2	8,026933E+0	65	0,67	0,51456
C32	2,804909E+1	2	8,045984E+1	65	11329,8	0,00000

Figure B.1 – Analysis of the adequacy of the clustering of the countries of the world into 2 and 3 groups as of 2021

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,377824E+0	3	3,656347E+0	64	0,80	0,49630
C1	6,263007E+0	3	1,706860E+0	64	0,78	0,507910
C2	3,250303E+0	3	8,504222E+0	64	0,82	0,490090
C3	1,231071E+0	3	1,367848E+0	64	1,92	0,135210
C4	1,231071E+0	3	1,367848E+0	64	1,92	0,135210
C5	4,152894E-0	3	1,202660E+0	64	0,74	0,534020
C6	4,648658E-0	3	2,923113E+0	64	3,38	0,023140
C7	3,148167E+1	3	9,651199E+1	64	6,96	0,000390
C8	4,380040E+0	3	3,483750E+0	64	2,68	0,054120
C9	3,451451E+0	3	7,805267E+0	64	0,94	0,425030
C10	1,780414E+0	3	2,923513E+0	64	1,30	0,282400
C11	2,435290E+0	3	1,371164E+0	64	0,38	0,768520
C12	6,861628E+0	3	7,527985E+0	64	1,94	0,131300
C13	2,530092E+0	3	7,955919E+0	64	0,68	0,568450
C14	2,553012E+0	3	2,014887E+0	64	2,70	0,052780
C15	4,152756E+0	3	8,197868E+0	64	1,08	0,363670
C16	2,188446E+0	3	2,874978E+0	64	0,16	0,921280
C17	5,077093E+0	3	1,659207E+0	64	0,65	0,584120
C18	6,317594E+0	3	2,651779E+0	64	0,51	0,678000
C19	2,769658E+1	3	3,826224E+1	64	15442,30	0,000000
C20	6,513978E+0	3	2,842471E+0	64	0,48	0,691220
C21	3,951691E+0	3	6,639638E+0	64	1,27	0,292300
C22	6,322340E+0	3	3,058225E+0	64	0,44	0,724450
C23	7,389435E+0	3	1,314981E+0	64	1,20	0,317390
C24	7,247216E+0	3	1,458879E+0	64	1,06	0,372470
C25	4,139202E+0	3	1,230796E+0	64	0,72	0,545200
C26	1,711106E+0	3	6,056843E+0	64	0,60	0,615630
C27	1,145833E+0	3	2,535379E+0	64	0,96	0,415200
C28	3,048386E+0	3	6,727457E+0	64	0,97	0,414010
C29	1,729964E+0	3	4,274484E+0	64	0,86	0,464750
C30	5,027242E+0	3	1,159879E+0	64	0,92	0,434050
C31	2,214148E+0	3	7,971311E+0	64	0,58	0,622130
C32	2,808384E+1	3	4,571356E+1	64	13106,00	0,000000

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	9,915237E+0	4	2,802606E+0	63	5,57	0,000660
C1	4,328112E+0	4	1,336679E+0	63	5,10	0,001260
C2	2,103521E+0	4	6,725731E+0	63	4,93	0,001610
C3	2,686614E+0	4	1,222294E+0	63	3,46	0,012770
C4	2,686614E+0	4	1,222294E+0	63	3,46	0,012770
C5	2,562020E-0	4	9,879866E-0	63	4,08	0,005240
C6	4,808147E-0	4	2,907164E+0	63	2,60	0,044070
C7	3,292040E+1	4	9,507326E+1	63	5,45	0,000770
C8	6,526762E+0	4	3,269077E+0	63	3,14	0,020180
C9	2,490463E+0	4	5,659949E+0	63	6,93	0,000100
C10	5,462855E+0	4	2,555269E+0	63	3,37	0,014640
C11	6,576926E+0	4	1,329748E+0	63	0,78	0,543030
C12	8,553826E+0	4	7,358765E+0	63	1,83	0,134000
C13	9,344749E+0	4	7,274453E+0	63	2,02	0,101880
C14	2,658657E+0	4	2,004322E+0	63	2,09	0,092700
C15	4,174901E+0	4	8,195653E+0	63	0,80	0,528280
C16	2,105299E+0	4	2,686332E+0	63	1,23	0,305420
C17	1,104775E+0	4	1,599500E+0	63	1,09	0,370240
C18	2,556917E+0	4	2,459263E+0	63	1,64	0,175890
C19	2,770464E+1	4	3,019629E+1	63	14450,30	0,000000
C20	4,557978E+0	4	2,451813E+0	63	2,93	0,027610
C21	1,077153E+0	4	5,957654E+0	63	2,85	0,031010
C22	2,082090E+0	4	2,913239E+0	63	1,13	0,352490
C23	3,721784E+0	4	1,016697E+0	63	5,77	0,000510
C24	2,566951E+0	4	1,274656E+0	63	3,17	0,019400
C25	1,270987E+0	4	1,145090E+0	63	1,75	0,150590
C26	5,620462E+0	4	5,665908E+0	63	1,56	0,195320
C27	3,835532E+0	4	2,266409E+0	63	2,67	0,040370
C28	1,058823E+0	4	5,973472E+0	63	2,79	0,033620
C29	2,175687E+0	4	4,229911E+0	63	0,81	0,523410
C30	9,618526E+0	4	1,113966E+0	63	1,36	0,257950
C31	5,332480E+0	4	7,659478E+0	63	1,10	0,366110
C32	2,809373E+1	4	3,581624E+1	63	12354,00	0,000000

Figure B.2 – Analysis of the adequacy of the clustering of the countries of the world into 4 and 5 groups as of 2021

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,246227E+0	5	2,547903E+0	62	6,07	0,00012
C1	4,358305E+0	5	1,333660E+0	62	4,05	0,00302
C2	2,224703E+0	5	6,604549E+0	62	4,18	0,00246
C3	3,322046E+0	5	1,158750E+0	62	3,55	0,00685
C4	3,322046E+0	5	1,158750E+0	62	3,55	0,00685
C5	2,666670E-0	5	9,775217E-0	62	3,38	0,00912
C6	4,898645E-0	5	2,898114E+0	62	2,10	0,07777
C7	3,373422E+1	5	9,425944E+1	62	4,44	0,00161
C8	7,465730E+0	5	3,175181E+0	62	2,92	0,01989
C9	2,213724E+0	5	5,936689E+0	62	4,62	0,00119
C10	6,817217E+0	5	2,419833E+0	62	3,49	0,00759
C11	3,436258E+0	5	1,361155E+0	62	0,31	0,90332
C12	1,128356E+0	5	7,085792E+0	62	1,97	0,09489
C13	5,618324E+0	5	7,647096E+0	62	0,91	0,47984
C14	2,717085E+0	5	1,998479E+0	62	1,69	0,15129
C15	7,197422E+0	5	7,893401E+0	62	1,13	0,35368
C16	1,586217E+0	5	2,738240E+0	62	0,72	0,61211
C17	9,043769E+0	5	1,619540E+0	62	0,69	0,63106
C18	1,683857E+0	5	2,546569E+0	62	0,82	0,54018
C19	2,770536E+1	5	2,948332E+1	62	11652,2	0,00000
C20	4,711025E+0	5	2,436508E+0	62	2,40	0,04722
C21	1,317070E+0	5	5,717738E+0	62	2,86	0,02196
C22	2,765683E+0	5	2,844880E+0	62	1,21	0,31717
C23	3,255260E+0	5	1,063349E+0	62	3,80	0,00460
C24	1,805729E+0	5	1,350778E+0	62	1,66	0,15825
C25	1,885164E+0	5	1,083672E+0	62	2,16	0,07032
C26	8,347569E+0	5	5,393197E+0	62	1,92	0,10384
C27	4,971460E+0	5	2,152816E+0	62	2,86	0,02170
C28	1,504769E+0	5	5,527526E+0	62	3,38	0,00923
C29	3,891543E+0	5	4,058326E+0	62	1,19	0,32492
C30	1,226015E+0	5	1,087550E+0	62	1,40	0,23751
C31	5,933254E+0	5	7,599400E+0	62	0,97	0,44433
C32	2,809618E+1	5	3,337154E+1	62	10439,8	0,00000

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,362426E+0	6	2,431704E+0	61	5,69	0,00009
C1	5,006469E+0	6	1,268843E+0	61	4,01	0,00189
C2	2,685303E+0	6	6,143949E+0	61	4,44	0,00086
C3	4,949343E+0	6	9,960207E+0	61	5,05	0,00029
C4	4,949343E+0	6	9,960207E+0	61	5,05	0,00029
C5	3,153091E-0	6	9,288795E-0	61	3,45	0,00532
C6	4,994590E-0	6	2,888520E+0	61	1,75	0,12296
C7	3,373591E+1	6	9,425775E+1	61	3,63	0,00375
C8	7,571854E+0	6	3,164568E+0	61	2,43	0,03571
C9	2,274789E+0	6	5,875623E+0	61	3,93	0,00217
C10	7,308445E+0	6	2,370710E+0	61	3,13	0,00961
C11	4,447652E+0	6	1,351041E+0	61	0,33	0,91601
C12	1,128385E+0	6	7,085763E+0	61	1,61	0,15725
C13	8,637083E+0	6	7,345220E+0	61	1,19	0,32089
C14	3,365181E+0	6	1,933670E+0	61	1,76	0,12049
C15	1,263361E+0	6	7,349782E+0	61	1,74	0,12526
C16	3,847176E+0	6	2,512145E+0	61	1,55	0,17524
C17	9,418542E+0	6	1,615792E+0	61	0,59	0,73496
C18	3,142598E+0	6	2,400695E+0	61	1,33	0,25739
C19	2,770564E+1	6	2,920329E+1	61	9645,28	0,00000
C20	6,401223E+0	6	2,267488E+0	61	2,87	0,01576
C21	1,668533E+0	6	5,366275E+0	61	3,16	0,00914
C22	4,576132E+0	6	2,663835E+0	61	1,74	0,12550
C23	3,396606E+0	6	1,049215E+0	61	3,29	0,00717
C24	1,955193E+0	6	1,335831E+0	61	1,48	0,19738
C25	3,146529E+0	6	9,575354E+0	61	3,34	0,00653
C26	1,521432E+0	6	4,706522E+0	61	3,28	0,00723
C27	8,604058E+0	6	1,789556E+0	61	4,88	0,00038
C28	2,522474E+0	6	4,509821E+0	61	5,68	0,00009
C29	5,563022E+0	6	3,891178E+0	61	1,45	0,20940
C30	1,935571E+0	6	1,016594E+0	61	1,93	0,08926
C31	1,272554E+0	6	6,920172E+0	61	1,87	0,10063
C32	2,809646E+1	6	3,308979E+1	61	8632,49	0,00000

Figure B.3 – Analysis of the adequacy of the clustering of the countries of the world into 6 and 7 groups as of 2021

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,480699E+0	7	2,313431E+0	60	5,486	0,000061
C1	5,509265E+0	7	1,218564E+0	60	3,875	0,00152
C2	3,054261E+0	7	5,774992E+0	60	4,533	0,00041
C3	5,633896E+0	7	9,275654E+0	60	5,206	0,00011
C4	5,633896E+0	7	9,275654E+0	60	5,206	0,00011
C5	3,969642E-0	7	8,472244E-0	60	4,016	0,00115
C6	6,212014E-0	7	2,766778E+0	60	1,924	0,08125
C7	3,373544E+1	7	9,425822E+1	60	3,066	0,00790
C8	7,640660E+0	7	3,157688E+0	60	2,074	0,06025
C9	2,225359E+0	7	5,925053E+0	60	3,215	0,00579
C10	6,986630E+0	7	2,402891E+0	60	2,492	0,02575
C11	4,249323E+0	7	1,353024E+0	60	0,265	0,96353
C12	1,249289E+0	7	6,964859E+0	60	1,537	0,17216
C13	7,439481E+0	7	7,464980E+0	60	0,854	0,54762
C14	2,741969E+0	7	1,995991E+0	60	1,177	0,32927
C15	1,168797E+0	7	7,444346E+0	60	1,346	0,24514
C16	4,249105E+0	7	2,471952E+0	60	1,473	0,19409
C17	9,071678E+0	7	1,619261E+0	60	0,480	0,84521
C18	4,659487E+0	7	2,249006E+0	60	1,776	0,10891
C19	2,770571E+1	7	2,913114E+1	60	8152,01	0,000001
C20	9,898358E+0	7	1,917774E+0	60	4,424	0,00051
C21	2,014668E+0	7	5,020139E+0	60	3,440	0,00369
C22	8,701147E+0	7	2,251333E+0	60	3,313	0,00478
C23	3,751589E+0	7	1,013717E+0	60	3,172	0,00637
C24	2,117654E+0	7	1,319585E+0	60	1,376	0,23230
C25	4,824692E+0	7	7,897191E+0	60	5,237	0,00010
C26	2,163391E+0	7	4,064563E+0	60	4,562	0,00039
C27	1,037925E+0	7	1,612037E+0	60	5,515	0,00006
C28	2,991767E+0	7	4,040528E+0	60	6,347	0,00001
C29	7,576031E+0	7	3,689877E+0	60	1,760	0,11235
C30	2,238997E+0	7	9,862514E+0	60	1,946	0,07786
C31	1,178562E+0	7	7,014164E+0	60	1,440	0,20637
C32	2,809650E+1	7	3,305543E+1	60	7285,55	0,000001

Variable	Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)					
	Between SS	df	Within SS	df	F	signif. p
C0	1,547563E+0	9	2,246566E+0	58	4,435	0,00019
C1	8,267302E+0	9	9,427602E+0	58	5,651	0,00001
C2	3,264428E+0	9	5,564824E+0	58	3,780	0,00084
C3	7,456275E+0	9	7,453274E+0	58	6,447	0,00000
C4	7,456275E+0	9	7,453274E+0	58	6,447	0,00000
C5	6,047376E-0	9	6,394510E-0	58	6,095	0,00000
C6	6,434175E-0	9	2,744561E+0	58	1,511	0,16585
C7	3,385201E+1	9	9,414166E+1	58	2,317	0,02651
C8	8,496207E+0	9	3,072133E+0	58	1,782	0,09131
C9	2,780213E+0	9	5,370199E+0	58	3,336	0,00238
C10	8,659767E+0	9	2,235578E+0	58	2,496	0,01738
C11	2,177737E+0	9	1,177743E+0	58	1,192	0,31778
C12	1,419450E+0	9	6,794697E+0	58	1,346	0,23394
C13	1,552973E+0	9	6,655955E+0	58	1,504	0,16841
C14	4,241292E+0	9	1,846058E+0	58	1,481	0,17687
C15	1,954086E+0	9	6,659058E+0	58	1,891	0,07135
C16	6,662434E+0	9	2,230619E+0	58	1,925	0,06606
C17	1,635934E+0	9	1,546384E+0	58	0,682	0,72215
C18	8,698961E+0	9	1,845059E+0	58	3,038	0,00481
C19	2,770620E+1	9	2,864323E+1	58	6233,62	0,000001
C20	1,496346E+0	9	1,411264E+0	58	6,833	0,00000
C21	2,493316E+0	9	4,541491E+0	58	3,538	0,00149
C22	1,160482E+0	9	1,960966E+0	58	3,814	0,00078
C23	5,767156E+0	9	8,121598E+0	58	4,576	0,00014
C24	4,617774E+0	9	1,069573E+0	58	2,782	0,00883
C25	6,424598E+0	9	6,297285E+0	58	6,575	0,00000
C26	2,968434E+0	9	3,259520E+0	58	5,865	0,00000
C27	1,406142E+0	9	1,243821E+0	58	7,285	0,00000
C28	4,113464E+0	9	2,918831E+0	58	9,082	0,00000
C29	1,103979E+0	9	3,343501E+0	58	2,128	0,04132
C30	2,973475E+0	9	9,128035E+0	58	2,095	0,04416
C31	1,668151E+0	9	6,524575E+0	58	1,648	0,12322
C32	2,809676E+1	9	3,278914E+1	58	5522,19	0,000001

Figure B.4 – Analysis of the adequacy of the clustering of the countries of the world into 8 and 10 groups as of 2021

Analysis of Variance (SpreadsheeBerezhna_dast_t.sta)						
Variable	Between SS	df	Within SS	df	F	signif. p
C0	1,757307E+0	10	2,036822E+0	57	4,91E	0,00004
C1	8,678101E+0	10	9,016803E+0	57	5,48E	0,00001
C2	3,870129E+0	10	4,959124E+0	57	4,44E	0,00012
C3	7,596990E+0	10	7,312560E+0	57	5,92E	0,00000
C4	7,596990E+0	10	7,312560E+0	57	5,92E	0,00000
C5	6,742018E-0	10	5,699868E-0	57	6,74E	0,00000
C6	6,759116E-0	10	2,712067E+0	57	1,42E	0,19488
C7	3,385255E+1	10	9,414110E+1	57	2,05E	0,04442
C8	8,486072E+0	10	3,073147E+0	57	1,57E	0,13807
C9	2,778826E+0	10	5,371586E+0	57	2,94E	0,00472
C10	9,547065E+0	10	2,146848E+0	57	2,53E	0,01331
C11	2,622587E+0	10	1,133258E+0	57	1,31E	0,24270
C12	1,355047E+0	10	6,859100E+0	57	1,12E	0,35950
C13	1,619283E+0	10	6,589645E+0	57	1,40E	0,20358
C14	4,345772E+0	10	1,835611E+0	57	1,34E	0,22746
C15	1,993436E+0	10	6,619708E+0	57	1,71E	0,09914
C16	6,519976E+0	10	2,244865E+0	57	1,65E	0,11436
C17	1,926479E+0	10	1,517330E+0	57	0,72E	0,69890
C18	8,709962E+0	10	1,843959E+0	57	2,69E	0,00897
C19	2,770625E+1	10	2,858825E+1	57	5524,14E	0,00000
C20	1,561060E+0	10	1,346550E+0	57	6,60E	0,00000
C21	2,441274E+0	10	4,593534E+0	57	3,02E	0,00386
C22	1,183245E+0	10	1,938203E+0	57	3,48E	0,00126
C23	6,060950E+0	10	7,827804E+0	57	4,41E	0,00013
C24	4,850034E+0	10	1,046347E+0	57	2,64E	0,01017
C25	6,438434E+0	10	6,283448E+0	57	5,84E	0,00000
C26	3,016414E+0	10	3,211540E+0	57	5,35E	0,00001
C27	1,417066E+0	10	1,232896E+0	57	6,55E	0,00000
C28	4,132771E+0	10	2,899524E+0	57	8,12E	0,00000
C29	9,951389E+0	10	3,452341E+0	57	1,64E	0,11773
C30	2,976557E+0	10	9,124954E+0	57	1,85E	0,07055
C31	1,669609E+0	10	6,523117E+0	57	1,45E	0,17903
C32	2,809685E+1	10	3,270324E+1	57	4897,13E	0,00000

Analysis of Variance (SpreadsheeBerezhna_clast_t.sta)						
Variable	Between SS	df	Within SS	df	F	signif. p
C0	1,774288E+0	11	2,019842E+0	56	4,47	0,00008
C1	7,044161E+0	11	1,065074E+0	56	3,37	0,00128
C2	3,981606E+0	11	4,847647E+0	56	4,18	0,00016
C3	6,607543E+0	11	8,302007E+0	56	4,05	0,00022
C4	6,607543E+0	11	8,302007E+0	56	4,05	0,00022
C5	5,084205E-0	11	7,357681E-0	56	3,52	0,00087
C6	7,294735E-0	11	2,658505E+0	56	1,40	0,20017
C7	1,186893E+1	11	9,304387E+1	56	64,94	0,00000
C8	9,101579E+0	11	3,011596E+0	56	1,54	0,14379
C9	3,213197E+0	11	4,937216E+0	56	3,31	0,00147
C10	7,786152E+0	11	2,322939E+0	56	1,71	0,09567
C11	1,259631E+0	11	1,269554E+0	56	0,51	0,89185
C12	1,602134E+0	11	6,612014E+0	56	1,23	0,28738
C13	1,283750E+0	11	6,925178E+0	56	0,94	0,50681
C14	3,374911E+0	11	1,932696E+0	56	0,85	0,55623
C15	1,437638E+0	11	7,175506E+0	56	1,02	0,44150
C16	5,177776E+0	11	2,379085E+0	56	1,11	0,37251
C17	1,850698E+0	11	1,524908E+0	56	0,62	0,80585
C18	7,066120E+0	11	2,008343E+0	56	1,79	0,07749
C19	2,772897E+1	11	5,867874E+1	56	24057,3	0,00000
C20	1,097093E+0	11	1,810517E+0	56	3,08	0,00267
C21	2,200262E+0	11	4,834545E+0	56	2,32	0,02005
C22	8,955821E+0	11	2,225866E+0	56	2,05	0,04029
C23	5,162156E+0	11	8,726598E+0	56	3,01	0,00324
C24	4,012050E+0	11	1,130146E+0	56	1,81	0,07442
C25	4,854531E+0	11	7,867352E+0	56	3,14	0,00231
C26	2,216074E+0	11	4,011880E+0	56	2,81	0,00546
C27	1,057034E+0	11	1,592928E+0	56	3,36	0,00124
C28	3,027492E+0	11	4,004803E+0	56	3,85	0,00037
C29	7,621930E+0	11	3,685287E+0	56	1,05	0,41483
C30	2,285334E+0	11	9,816176E+0	56	1,15	0,31824
C31	1,198610E+0	11	6,994115E+0	56	0,87	0,57148
C32	2,812225E+1	11	7,304525E+1	56	19599,8	0,00000

Figure B.5 – Analysis of the adequacy of the clustering of the countries of the world into 11 and 12 groups as of 2021

Summary Statistics; DV: C0 (SpreadsheetBerezhna_fact_5)	
Statistic	Value
Multiple R	0,9056
Multiple R?	0,82014
Adjusted R?	0,7809
F(12,55)	20,8996
p	0,0000
Std.Err. of Estimate	11,1388

Figure B.5 – Analysis of the adaptations of the clustering of the countries of the world into 11 and 12 groups as of 2021

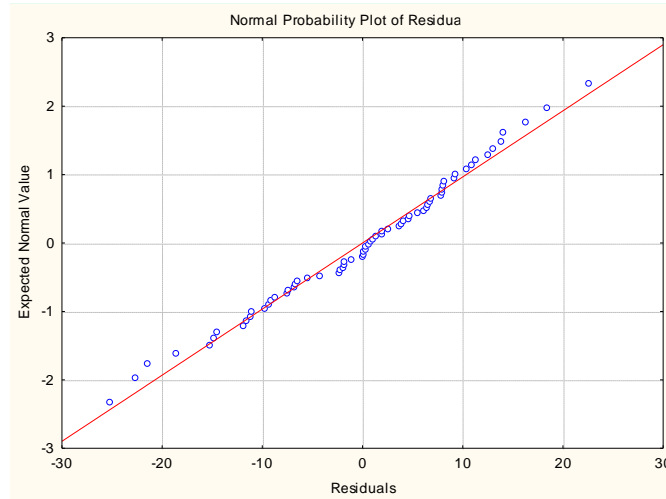


Figure B.7 – Graphic representation of compliance with the normal law of the distribution of the residuals of the linear regression model of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for 68 countries of the world (32 factors)

Summary Statistics; DV: C0 (SpreadsheetBerezhna_fact_...	
Statistic	Value
Multiple R	0,87543
Multiple R ²	0,76638
Adjusted R ²	0,74754
F(5,62)	40,67841
p	0,00000
Std.Err. of Estimate	11,95671

Figure B.8 – Indicators of the adequacy of the regression analysis of the dependence between the level of cyber security and the factors determining the state of combating financial cyber fraud for 68 countries of the world (5 factors)

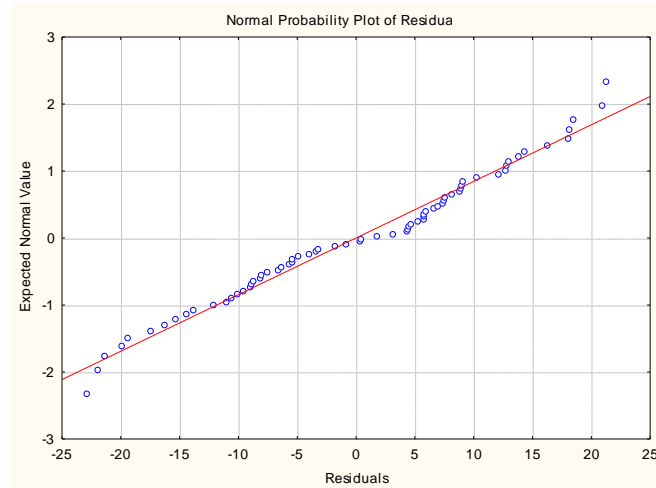


Figure B.9 – Graphic representation of compliance with the normal law of the distribution of the residuals of the linear regression model of the dependence between the level of cyber security and relevant factors that determine the state of combating financial cyber fraud for 68 countries of the world (5 factors)

Summary Statistics; DV: C0 (SpreadsheetBerezhna_fact_cl3.k	
Statistic	Value
Multiple R	1,000000
Multiple R?	1,000000
Adjusted R?	1,000000
F(6,0)	
p	
Std.Err. of Estimate	0,000000

Figure B.10 – Indicators of the adequacy of the regression analysis of the dependence between the level of cyber security and the factors that determine the state of combating financial cyber fraud for the cluster of 7 countries with Ukraine (32 factors)

Members of Cluster Number 1 and Distances from Respective Cluster contains 6 cases	
	Distance
Germany	376848,
Italy	98244,
Mexico	58717,
Spain	126385,
Türkiye	113507,
Vietnam	70603,

Members of Cluster Number 2 and Distances from Respective Cluster contains 1 cases	
	Distance
China	0,00

Members of Cluster Number 4 and Distances from Respective Cluster contains 9 cases	
	Distance
Belgium	192211,
Chile	51550,
Czech Republic	141494,
Greece	108735,
Hungary	233700,
Malaysia	145143,
Portugal	86973,
Sweden	73853,
Uzbekistan	582865,

Members of Cluster Number 5 and Distances from Respective Cluster contains 13 cases	
	Distance
Austria	87414,
Belarus	179958,
Bulgaria	68478,
Denmark	361580,
Finland	97900,
Ireland	161440,
Israel	158218,
Morocco	160971,
Pakistan	183324,
Peru	229237,
Slovakia	123098,
South Africa	160356,
Sri Lanka	212408,

Figure B.11 – Composition and characteristics of the 1st, 2nd, 4th, 5th out of 9 conditional clusters of countries of the world in terms of the level of cyber security and the state of combating financial cyber fraud according to the Euclidean distance indicator

Members of Cluster Number 6 and Distances from Respective Cluster contains 6 cases		Members of Cluster Number 7 and Distances from Respective Cluster contains 7 cases	
	Distance		Distance
Costa Rica	41642,4	Albania	37324,7
Croatia	28066,4	Dominican Republic	57635,2
Georgia	23331,4	Jordan	16518,6
Senegal	184129,4	Moldova (Republic of)	35552,8
Tunisia	89963,4	Myanmar	38345,4
Uruguay	31545,0	Panama	26421,1
		Slovenia	28405,4

Members of Cluster Number 8 and Distances from Respective Cluster contains 11 cases		Members of Cluster Number 9 and Distances from Respective Cluster contains 8 cases	
	Distance		Distance
Cambodia	7149,9	Botswana	17730,1
Cameroon	43684,6	Madagascar	12272,9
Cyprus	13717,2	Malawi	15499,8
Honduras	9736,4	Mali	7895,2
Jamaica	19129,7	Mozambique	6284,1
Latvia	31143,6	Nigeria	6333,7
Luxembourg	23980,6	Zambia	4279,1
Malta	28816,6	Zimbabwe	18163,0
Mauritius	8585,9		
Mongolia	5594,3		
Trinidad and Tobago	3421,2		

Figure B.12 – Composition and characteristics of the 6th, 7th, 8th, and 9th out of 9 conditional clusters of the countries of the world in terms of the level of cyber security and the state of combating financial cyber fraud according to the Euclidean distance indicator

APPENDIX C



Міністерство освіти і науки України

**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ХІМІКО-ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ»**

просп. Гагаріна, 8, Дніпро, 49005, Україна

Телефон: (056) 746-33-56, факс: (056) 746-26-68, E-mail: udhtu@udhtu.edu.ua, Код ЄДРПОУ 02070758

№ _____

на № _____

Повідомляємо, що редакційною колегією наукового фахового видання «Економічний вісник «Державного вищого навчального закладу «Український державний хіміко-технологічний університет» розглянуто та рекомендовано до друку статтю ДОЦЕНКО Тетяни, ЯРОВЕНКО Ганни, БЕРЕЖНОЇ Дарини «Due diligence в аспекті протидії фінансовим кібершахрайствам: тенденції моделювання»/ Dotsenko Tetiana, Yarovenko Hanna, Berezhna Darina «Due diligence in the aspect of countering financial cyber fraud: modeling trends».

Стаття буде опублікована в 1 (17) номері 2023 року збірника наукових праць «Економічний вісник Державного вищого навчального закладу «Український державний хіміко-технологічний університет».

Наказом Міністерства освіти і науки України від 17.03.2020 № 409 «Про затвердження рішень Атестаційної колегії Міністерства щодо формування Переліку наукових фахових видань України від 26 лютого і 6 березня 2020 року та внесення змін до наказу Міністерства освіти і науки України від 11 липня 2019 року № 975» збірник наукових праць «Економічний вісник ДВНЗ «Український державний хіміко-технологічний університет» включено до категорії «Б» Переліку наукових фахових видань України.

З 2016 року збірник наукових праць індексується міжнародною наукометричною базою Index Copernicus, ICV 2018: 67.87; 2019: 80.79; 2020: 75.32; 2021:68.75.

Головний редактор видання
«Економічний вісник ДВНЗ УДХТУ»



Лариса ГАРМІДЕР

Секретар видання
«Економічний вісник ДВНЗ УДХТУ»



Олена ЧЕРНИШЕВА