UDC 336.7:338.24]:004.056.5
JEL Classification: K00, G00, G24

Dotsenko Tetiana [ab*], Yarovenko Hanna [a], Berezhna Darina [a]

DUE DILIGENCE IN THE ASPECT OF COUNTERING FINANCIAL CYBER FRAUD: MODELING TRENDS

[a] Sumy State University, Sumy, Ukraine
[b] Technical University of Berlin, Berlin, Germany

The article emphasizes that financial cyber frauds pose a significant risk to the financial and economic security and stability of modern business entities. It was emphasized that in order to prevent fraud, in order increase the efficiency of economic activity, it is necessary to introduce a system of reliable protection of subjects based on the application of various mechanisms and tools, which include proper verification of the functioning of enterprises. Goal of the study is to determine the latest trends in modeling the fight against financial cyber fraud based on the Due Diligence methodology. The relevance of determining the latest trends in the modeling of combating financial cyber-fraud is that the study of the financial protection system, including through the application of such a verification procedure as Due diligence, will contribute to the improvement of the financial cyber protection of the enterprise. The interpretation of the concept of due diligence has been formed, its normative basis has been outlined, a number of stages and features have been developed regarding the implementation of due diligence, a structural and logical scheme of the stages and features of the implementation of due diligence of enterprises has been built. Modern methods of modeling due diligence and modeling approaches for countering financial cyber fraud are described. The advantages of the implementation of the complex Due Diligence methodology in the aspect of combating financial cyber fraud for enterprises have been determined. Theoretical research methods - empirical research methods - observation, description; grouping, abstraction; the resource base of the information platform; Bizagi Modeler software. The obtained results of the research can be practically used at enterprises for the formation of guiding principles and policies for the 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.

Keywords: Due diligence, financial fraud, combating financial cyber fraud, modeling, data mining methods.

DOI: 10.32434/2415-3974-2022-17-1-20-30

Introduction and formulation of the problem

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, the improper activity of the institution, deficiencies in information and technical support, and 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 entities 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, and due diligence procedures.

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 has been decisive in the activities of enterprises in recent years, a system of financial cyber protection is emerging. And to counter 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 a 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.

Analysis and research of publications

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., Hrzic R. regarding the impact and consequences of the European Union Law on Due Diligence on the activities of small businesses; Deva S., Villiers C., Liesa C.R.F., Sedano T.G. regarding discussions of legislative and legal issues Due diligence; Litwin D. regarding due diligence of economic inequality, the impact of business on inequality; Guanipa H.J., Chima J.T., Camoletto S., Corazza L., Pizzi S., Santini E. 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: 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. [1]; predict information trends for countering cybercrime risks Kuzior A., Broïek P., Kuzmenko O., Yarovenko H., Vasilyeva T. [2]; they are conducting an evolutionary study of approaches to combating financial cybercrime Nicholls J., Kuppa A., Le-Khac N.; study the features of combating fraud caused by technology Dadhich M., Hiran K.K., Rao S.S., Sharma R., Meena R.; on the investigation of cybercrimes Bello M., Griffiths M.; 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. describe the application of the due diligence procedure due diligence of objects to manage the risks of corporate economic security; Chitimira H., Munedzi S. 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., Shutaywi M., Alsenani T.R.; information modeling (information analysis) – Lu T., Wang C., Cao Y., Chen H.; economic modeling – Botchway S., Tsiachristas A., Pollard J., Fazel S.; structural modeling – 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.; and many others.

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., Ziyiko A., Kuzmenko O., Kapinos A., Humenna Y. [3] – 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., Suler P., Lyeonov S., Judrupa I., Boiko A. [4] – 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., Rio-Belver R.M., Alvarez-Meaza I. – apply a new approach to combining social network analysis methods with the use of artificial neural network models; Kumagai A., Jeong S., Kim D., Kong H., Oh S., Lee S. – describe the application of intelligent data analysis models to analyze the

effectiveness and accuracy of medical tests; Ren D., Wang C., Wei X., Lai Q., Xu W. – 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., Forte S., & Melisi G. [5] propose a due diligence model based on machine learning; Roy V., Desjardins D., Fertel C., Ouellet-Plamondon C. [6] developed a due diligence model based on risk assessment; Aman A., & Reji D.J. [7] reveal the features of building a due diligence model based on deep learning of NLP; Li Z. [8] 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., Yuksel S., Dinзer H. [9] interpret the model of consensus multidimensional verification of investment projects based on financial technologies; Liu Y., Feng Y., Zhou B. [10] ropose 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. 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. [11] 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., Brozek P. [12] 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., Kubalek J., Bozhenko V.V., Kushneryov O.S., Vida, I. [13] highlight Machine Linked Learning (SVM) models for protecting the financial sector from cybercrime; Wahid S.D.M., Buja A.G., Hasrol Jono M.N.H., Aziz A.A. [14] propose the application of an assessment model for assessing the influential factors of cyber security awareness; Buja A.G., Wahid S.D.M., Rahman T.F.A., Deraman N.A., Jono M.N.H.H., Aziz A.A. [15] 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 comprehensive, reliable, effective approaches to evaluating the activities of business entities in terms of the policy of protection against financial cyberattacks.

Purpose of the article

The main purpose of the study is to determine the latest trends in modeling the fight against financial cyber fraud based on the Due Diligence methodology.

Presentation of the main material

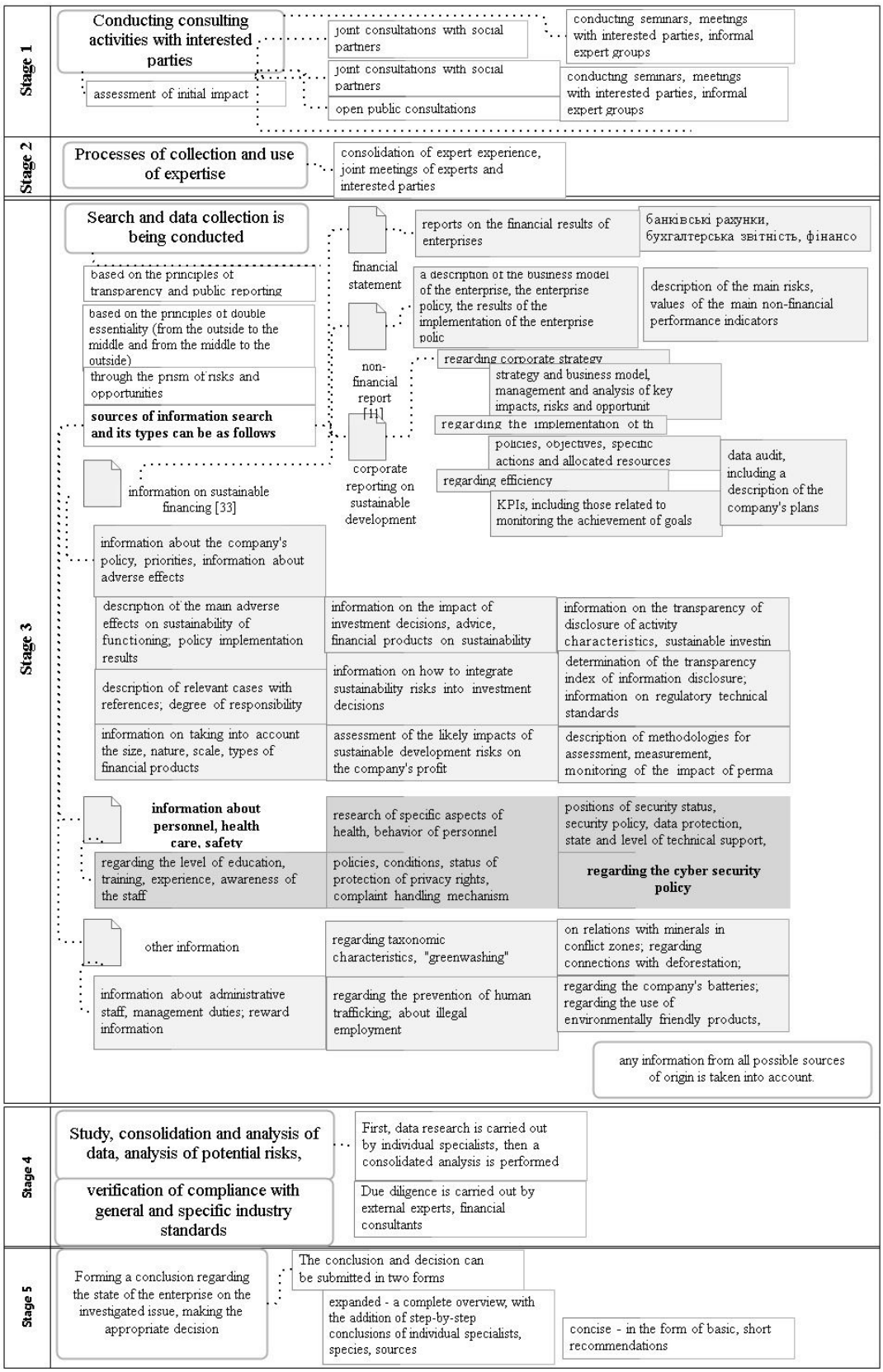
After analyzing the literature on the researched issue, the concept of Due Diligence (due diligence, expertise) was formulated – as a scientific category that involves a complex of actions: multi-vector research and assessment of the subject's work, with an in-depth study of the financial condition, assessment of risks (including financial , investment), analysis of the location of the object 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.

The regulatory basis for due diligence is the Proposal for the Directive of the European Parliament and the Council on Corporate Sustainability Due Diligence dated February 23, 2022. The European Union's Due Diligence Act is aimed at achieving the UN's sustainable development goals, particularly in areas related to human rights and the environment, security, and mitigating negative impacts on them. What will allow to form effective business solutions to protect organizations, ensure long-term sustainability of enterprises.

Due Diligence, among other things, allows you to determine and form an understanding of the state of financial protection of the subject of the study, in particular, its financial cyber security, to ensure measures against financial crimes and financial cyber fraud. To carry out due diligence of enterprises in the aspect of combating financial cyber fraud, it is advisable to define a number of stages and features of its conduct. Figure shows the structural and logical scheme of the stages and features of conducting a proper inspection of the enterprises built during the study. The scheme is built using Bizagi Modeler software.

But an important component of assessing the functioning of enterprises is the modeling of such due diligence processes described above.

1. Due diligence model based on machine learning [5] involves assessing the profitability of



Structural and logical scheme of stages and features of due diligence implementation of enterprises

Source: developed by the authors

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 (data on the bank's problem loans market, the value of the portfolio of problem loans, the risk percentage of the level of reimbursement); modeling complex relationships between predictors and variables using ML algorithms; assessment of the profitability of transactions using due diligence (estimation of the expected return of interest on outstanding mortgage loans); 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):

$$K = \sqrt{VL \cdot VR} \cdot \left| rVL - rVR \right|, \quad (1)$$

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.

Then the nonlinear correlation will have the form (formula 2):

$$R = SSQ(a - bH), \quad (2)$$

where r is a non-linear correlation; SSQ – sum of squares; a – undefined variable; bH – weighted sum of data set variables.

Next, an approach to pricing a portfolio of problematic loans on the secondary market is formulated (formula 3).

$$VPPL = E[PVECF, i(0,t)] - CC, \quad (3)$$

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 [6] 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 [7] 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 (manual selection of raw text data from the EPA website, secondary data from the Mendeley repository); 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 [8]. 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 (legal obligations for specific types of business, procedural standards, areas of activity, legal sanctions for non-compliance and violations). 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 [9] 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 4)

$$X = \begin{bmatrix} 0 & x12 & x13 & \dots & x1n \\ x21 & 0 & x23 & \dots & x2n \\ x31 & x32 & 0 & \dots & x3n \\ \dots & \dots & \dots & \dots & \dots \\ xn1 & xn2 & xn3 & \dots & 0 \end{bmatrix}, \quad (4)$$

where X is the direct connection matrix; normalization of the direct connection matrix (formula 5)

$$Y = \frac{X}{\max_{1 \le i \le n} \sum_{j=1}^{n} xij}, \quad (5)$$

where U is the normalization of the direct connection matrix; formation of the general ratio matrix; calculation of the limit value; forming conclusions.

6. A computer model of due diligence through AHP and big data [10] involves quantifying current technical due diligence. The model includes the following stages: formation of the research information base (determination of key indicators of the first level – equipment, environmental protection, energy saving, management); 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 6), performing consistency testing;

$$T=Aen \cdot Ben+Aeq \cdot Beq+Aes \cdot Bes+Am \cdot Bm, \quad (6)$$

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 (effectively increasing the level and efficiency of technical inspection; significant reduction of investment risk).

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 [11] 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 (age, socio-

professional category, marital status, household situation, household composition, difficulties with paying bills, class membership, subjective urbanization, Internet use, familiar devices, Internet access, awareness of the existence of portals/forms for reporting cybercrime); 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) [12]. 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 (selection of countries for research; determination of the research period; selection of indicators for the model – level of national cyber security, ease of obtaining electricity, ease of doing business, anti-money laundering index, level of digital development of the country; formation indicators of digital development - the number of Internet users, people with advanced qualifications, infrastructure indicators (network coverage, population covered by a 3G mobile network, population covered by a 4G mobile network), access (access to ICT at home, active subscription to mobile broadband, fixed broadband subscription), 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 7) using indicators of digital development

$$Kv = \frac{Sd}{m} \cdot 100\% = \frac{\sqrt{\sum_{i=1}^{n} \frac{(a_i - m)^2}{(n-1)}}}{\frac{\sum_{i=1}^{n} a_i}{n}}, \quad (7)$$

where Kv is the coefficient of variation, Sd is the standard deviation, m is the average value, n is the number of data points, a_i is 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 (normalization of indicators, calculation of correlation coefficients using Spearman's rank correlation coefficients in the Statgraphics 19 application program; construction econometric regression models, checking the statistical significance of the model based on the Student's test, the level of significance p – value, R-squared, the Durbin-Watson test); development of quantile regression models (determining estimates of regression coefficients for quantiles based on nonlinear optimization using the gradient descent method; estimation of model error by using the covariance matrix and nuclear estimation of the density of errors; calculation of the standard error, Student's test, and the significance level of the p-value using the values of the covariance matrix, taking into account kernel of estimation of model error density); forming 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 (the existence of a significant correlation between the factors of online financial activity and cyberattacks; the presence of a significant influence of the factors of digital skills on the fight against cyberattacks); 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 8)

$$Ikn = \sum_{j=1}^{j} \sum_{j=1}^{j} \left(sn_j\right)^2, \quad (8)$$

where Ikn is the integral index of cyber threats in the section of the nth country, sn_j – the standardized value of the jth indicator of the spread of cyber threats in the section of the nth country; identification of potential drivers of cyber threats (internet user skills, people who have used the internet to use online banking services, online activity, mobile broadband index, advanced skills and development, business digitization); implementation of the construction of two types of SVM machine learning models (epsilon-SVM regression and nu-SVM regression) using the Statistica statistical analysis software package, different types of functional dependence between variables (linear, radial basis, polynomial, sigmoidal) were constructed by applying the reference vector method (formula 9)

$$f = \begin{Bmatrix} a_i \cdot a_j & \text{linear type} \\ \exp\left(-h \cdot \left(a_i - a_j\right)^2\right) & \text{radial basis type} \\ \left(h \cdot a_i \cdot a_j + c\right)^p & \text{polynomial type} \\ \tanh\left(h \cdot a_i \cdot a_j + c\right) & \text{sigmoid type} \end{Bmatrix}, \quad (9)$$

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

4. Scoring Models for Assessing the Influential Factors of Cybersecurity Awareness [14] 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 (security training, awareness raising program, information security policy, information security culture), social (media influence, family and friends, public administration) and individual (personal initiative, knowledge of information systems, security training) influence on cyber security awareness); data analysis (measurement and scaling of the theoretical construct; SEM evaluation – confirmatory factor analysis (CFA) testing); measurement model testing (measurement model analysis; convergent validity and composite reliability analysis; discriminant validity analysis); testing structural model (hypothesis testing), CMV (common method variance) testing, formation of research conclusions.

5. A Cybersecurity Awareness Model for Seniors [15] 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.

Conclusions

The results of the study show that the modernization of the processes of ensuring financial, and especially cyber security of enterprises, is becoming a priority direction for the management of modern business entities. This will help ensure an effective policy against financial threats and risks. Moreover, an effective tool for countering financial cyber fraud is the application of due diligence processes of enterprises, as the latest system for checking the state of the subject's activity.

In contrast to such methods of financial checks as audit, audit, observation, inspection, analysis, examination, which are widely used for financial checks of the activities of enterprises, due diligence is a more complex and systematic approach. It helps to more fully understand the potential risks and benefits. This type of audit allows for a more detailed investigation of the research question, such as financial cyber fraud. The advantages of due diligence include: better decision-making, reduction of risks, improvement of negotiations on investment issues. Although the disadvantages of this method should be noted: it takes a lot of time, usually requires additional costs, the possibility of incomplete information. So, although due diligence procedures take a lot of time and are expensive, they help the management to make more reasonable and, accordingly, more effective decisions, to reduce risks.

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

The work was performed within the scope of the research topic «Data-Mining for countering cyber fraud and legalization of criminal proceeds in the conditions of digitalization of the financial sector of the economy of Ukraine «, state registration number: 0121U100467; «Modeling the mechanisms of detinization and decorruption of the economy to ensure national security: the impact of the transformation of financial behavioral patterns», state registration number: 53.16.01-22/24.3П-01; the topic «National security through the convergence of financial monitoring systems and cyber security: intelligent modeling of financial market regulation mechanisms» state registration number: 0121U109559.

The article was written during a research stay at the Technical University of Berlin, Department of Health Care Management.

REFERENCES

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

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

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

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

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

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

7. Aman, A., & Reji, D. J. (2022). Environmental due diligence data: A novel corpus for training environmental domain NLP models. *Data in Brief, 45.* doi:10.1016/j.dib.2022.108579.

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

9. Liu, W., Sun, Y., Yuksel, S., & Dincer, H. (2021). Consensus-based multidimensional due diligence of fintech-enhanced green energy investment projects. *Financial Innovation, 7(1).* DOI:10.1186/s40854-021-00289-3.

10. Liu, Y., Feng, Y., & Zhou, B. (2021). Research on due diligence computer model of thermal power plant considering through AHP and big data. *Journal of Physics: Conference Series, 2033(1).* DOI:10.1088/1742-6596/2033/1/012061.

11. Vasilyeva, T. A., Kuzmenko, O. V., Stoyanets, N. V., Artyukhov, A. E., & Bozhenko, V. V. (2022). Pobudova portretu kiberderzhavy z vykorystanniam tekhnolohiy data-mining [The depiction of cybercrime victims using data mining techniques]. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (5), 174-178. DOI:10.33271/nvngu/2022-5/174 [in Ukrainian].

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

13. Kuzmenko, O. V., Kubalek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. *Polish Journal of Management Studies, 24(2),* 276-291. DOI:10.17512/pjms.2021.24.2.17.

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

15. Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). Development of organization, social and individual cyber security awareness model (osicsam) for the elderly. International Journal of Advanced Technology and Engineering Exploration, 8(76), 511-519. doi:10.19101/IJATEE.2020.762185.

Received 03.04.2023

DUE DILIGENCE В АСПЕКТІ ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ: ТЕНДЕНЦІЇ МОДЕЛЮВАННЯ

Доценко Т. В., Яровенко Г. М., Бережна Д. Є.

У статті підкреслено, що фінансові кібершахрайства становлять значний ризик для фінансово-економічної безпеки і стабільності сучасних суб'єктів господарювання. Наголошено, що для перешкоджання шахрайствам, з метою підвищення ефективності господарської діяльності, необхідно запроваджувати систему надійного захисту суб'єктів на основі застосування різних механізмів та інструментів, що включають належну перевірку функціонування підприємств. Мета дослідження – визначення останніх тенденцій моделювання протидії фінансовим кібершахрайствам на основі методики Due diligence. Актуальність визначення останніх тенденцій моделювання протидії фінансовим кібершахрайствам полягає в тому, що дослідження системи фінансового захисту, в тому числі через застосування такої процедури перевірки як Due diligence, сприятиме підвищенню фінансового кіберзахисту підприємства. Сформовано трактування поняття due diligence, окреслено його нормативну основу, розроблено низку етапів і особливостей щодо реалізації Due diligence, побудовано структурно-логічну схему етапів і особливостей реалізації Due diligence підприємств. Описано сучасні методики моделювання due diligence та підходи моделювання протидії фінансовим кібершахрайствам. Визначено переваг впровадження комплексної методики Due diligence в аспекті протидії фінансовим кібершахрайствам для підприємств. Методичним інструментарієм використано теоретичні методи дослідження – емпіричні методи дослідження – спостереження, опис; групування, абстрагування; ресурсна база інформаційної платформи; ПЗ Bizagi Modeler. Отримані результати дослідження можуть бути практично використані на підприємствах для сформування керівних принципи та політики фінансової безпеки підприємств, що в свою чергу допоможе знизити рівень негативних наслідків в тому числі і фінансових кіберзагроз, фінансових кіберризиків, що можуть

бути присутні у бізнес процесах; максимізувати можливі позитивні ефекти від прийняття сформованих з урахуванням низки факторів, управлінських рішень.

Ключові слова: Due diligence, фінансові шахрайства, протидія фінансовим кібершахрайствам, моделювання, методи data mining.

DUE DILIGENCE IN THE ASPECT OF COUNTERING FINANCIAL CYBER FRAUD: MODELING TRENDS

Dotsenko Tetiana [ab*], Yarovenko Hanna [a], Berezhna Darina [a]

[a] Sumy State University, Sumy, Ukraine

[b] Technical University of Berlin, Berlin, Germany

[*]e-mail: t.dotscenko@uabs.sumdu.edu.ua

Dotsenko Tetiana ORCID: **http://orcid.org/0000-0001-5713-2205**

Yarovenko Hanna ORCID: **http://orcid.org/0000-0002-8760-6835**

Berezhna Darina ORCID: **http://orcid.org/0009-0008-8995-6602**

The article emphasizes that financial cyber frauds pose a significant risk to the financial and economic security and stability of modern business entities. It was emphasized that in order to prevent fraud, in order increase the efficiency of economic activity, it is necessary to introduce a system of reliable protection of subjects based on the application of various mechanisms and tools, which include proper verification of the functioning of enterprises. Goal of the study is to determine the latest trends in modeling the fight against financial cyber fraud based on the Due Diligence methodology. The relevance of determining the latest trends in the modeling of combating financial cyber-fraud is that the study of the financial protection system, including through the application of such a verification procedure as Due diligence, will contribute to the improvement of the financial cyber protection of the enterprise. The interpretation of the concept of due diligence has been formed, its normative basis has been outlined, a number of stages and features have been developed regarding the implementation of due diligence, a structural and logical scheme of the stages and features of the implementation of due diligence of enterprises has been built. Modern methods of modeling due diligence and modeling approaches for countering financial cyber fraud are described. The advantages of the implementation of the complex Due Diligence methodology in the aspect of combating financial cyber fraud for enterprises have been determined. Theoretical research methods - empirical research methods - observation, description; grouping, abstraction; the resource base of the information platform; Bizagi Modeler software. The obtained results of the research can be practically used at enterprises for the formation of guiding principles and policies for the 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.

Keywords: Due diligence, financial fraud, combating financial cyber fraud, modeling, data mining methods.

REFERENCES

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

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

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

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

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

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

7. Aman, A., & Reji, D. J. (2022). Environmental due diligence data: A novel corpus for training environmental domain NLP models. *Data in Brief, 45.* doi:10.1016/j.dib.2022.108579.

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

9. Liu, W., Sun, Y., Yuksel, S., & Dincer, H. (2021). Consensus-based multidimensional due diligence of fintech-enhanced green energy investment projects. *Financial Innovation, 7(1).* DOI:10.1186/s40854-021-00289-3.

10. Liu, Y., Feng, Y., & Zhou, B. (2021). Research on due diligence computer model of thermal power plant considering through AHP and big data. *Journal of Physics: Conference Series, 2033(1).* DOI:10.1088/1742-6596/2033/1/012061.

11. Vasilyeva, T. A., Kuzmenko, O. V., Stoyanets, N. V., Artyukhov, A. E., & Bozhenko, V. V. (2022). Pobudova portretu kiberderzhavy z vykorystanniam tekhnolohiy data-mining [The depiction of cybercrime victims using data mining techniques]. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (5), 174-178. DOI:10.33271/nvngu/2022-5/174 [in Ukrainian].

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

13. Kuzmenko, O. V., Kubalek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. *Polish Journal of Management Studies, 24(2),* 276-291. DOI:10.17512/pjms.2021.24.2.17.

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

15. Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). Development of organization, social and individual cyber security awareness model (osicsam) for the elderly. International Journal of Advanced Technology and Engineering Exploration, 8(76), 511-519. doi:10.19101/IJATEE.2020.762185.