ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 95

6th International Conference on Strategies, Models and Technologies of Economic Systems Management (SMTESM 2019)

Modeling of Risks and Threats in the Management of Personnel Security of the Enterprise

Tetiana Zatonatska
Department of Economic Cybernetics
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
tzatonat@ukr.net

Olena Liubkina
Department of Finance
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
Lev2373@ukr.net

Dmytro Zatonatskyi
PhD student
National Institute for Strategic Studies
Kyiv, Ukraine
dzatonat@gmail.com

Maksym Bilychenko
Student of the Faculty of Economics
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
mbilich9@gmail.com

***Abstract*—The article outlines the author's model of risks and threats prediction as components of a comprehensive system of personnel safety management at an enterprise based on the application of the psychosocial approach. It is proved that the psychological features and behavior of employees may form the basis of such a model as the most significant factors in the formation of a safe personnel situation at the enterprise. The strengths and weaknesses of the Bayesian network, which today is widespread and at the same time promising methodical tool for modeling processes with uncertainties of arbitrary nature, are determined. The possibility and feasibility of adopting the Bayesian model in determining the probability of personnel hazards arising from the employees of the enterprise is justified. A step-by-step scenario for applying the Bayesian network using the results of expert assessments that have received verifiability has been presented. An algorithm for introducing a psychosocial approach to personnel risk assessment at an enterprise has been developed. It is emphasized that the model developed by the authors can be introduced into the practice of assessing the psychosocial potential of employees, which will allow not only to identify threats to human security, but also to set directions in improving the motivation mechanisms as a precondition for the enhancing of personnel security.**

Keywords—personnel security, economic security, modeling of personnel hazards risks, models of diagnosing threats to personnel security.

I. INTRODUCTION

New challenges caused by the nature of the behavioral economy with the dominant psychological peculiarities of human perception of socio-economic realities of the present, highlight the issues of personnel security of enterprises. In such conditions, the growing need for introducing a number of organizational and economic measures that would protect the enterprise from the risks of loss of official and professional secrets and harming caused not only due to lack of competence and motivation of staff, but also because of the psychological inclination to create threats of disequilibrium in the personnel field of activity of enterprises. The use of modern approaches and models of diagnosis of personnel hazards risk based on the analysis of behavior, which is caused by the psychological characteristics of the individual and its place and perception in society, can identify employees who are carriers of threats to personnel security of the enterprise. Therefore, losses caused by violations of the economic security system due to the sources of confidential information can be prevented and the behavior of workers can be corrected before the negative factor becomes critical.

II. ANALYSIS OF THE LATEST RESEARCH, IN WHICH THE PROBLEM-SOLVING WAS INITIATED

The problem of personnel security management with the use of tools for psychosocial diagnostics was reflected in the research of such scholars as [1] - [5]. Modeling of risk indicators for personnel hazards using a psychological approach is considered in the papers [6], [7].

For the scientific position of the above-mentioned researchers, the assumption is made about the possibility of predicting the behavior of the personnel, which may pose a threat to the enterprise (due to the unauthorized transmission of confidential data), on the basis of an analysis of their mental and emotional state. There is a sufficient number of scientific studies devoted to assessing the relationship between the origin of the risks and motives of the insiders and certain characteristics of the employee's behavior [1] - [3].

A new conceptualization that is greatly based on case studies of internal threats and psychological theory was proposed in the work of Burse et al. (2014) [8]. This structure points out several key elements in the problem space, focusing not only on events and technical and behavioral indicators which merit attention, but also on the intruders (e.g. motivation for malicious threats and human factors related to unintentional one) and on the range of attacks. This can serve as a framework for a common understanding of the threat, as well as for modeling past and potential future attacks on the personnel security of an enterprise. The results of this work highlight the importance of the influence of the current psychological state of the insider worker on the motivation and attitude to attack.

Furthermore, researchers emphasize the fact of personal characteristics that merits attention when detecting intruders. Among the various personality traits, it was found that "machiavellianism", the desire to violation, and narcissism, are most related to the problems of internal threat.

An online system of deep learning without a teacher, which allows to reveal a threat to personnel security in complex data flows is presented in a research paper by Tuor et al (2012) [9]. This model is constantly being studied online to adapt to changing conditions and to discover new patterns in data flows. The model proposed in this work uses deep neural networks and recurrent neural networks to study and evaluate whether user behavior is normal. During data processing, data are not cached endlessly, and decisions are made as quickly as new data arrive in a neural network model. The evaluation of this model and its productivity exceeded some other existing methods of abnormality detection. However, the possibility to skip abnormal patterns that occur within one day is one of the limitations of this model.

One of the most common management practices used to identify personality and a behavioral characteristic is a five-factor questionnaire ("Big Five"), developed by American psychologists R. McCrae and P. Costa [10]. This test is a set of 75 pairs, opposite in its meaning, statements that characterize human behavior. With the help of this test, it is possible to determine precisely the type of human behavior, namely indicators that are part of the OCEAN model (emotional stability, extraversion, openness to experience, cooperation and conscientiousness). Dissatisfaction in the workplace and employee dissatisfaction in the scientific work of Willison [2] received the argumentation of the main causes of organizational crime according to the work. Workman's work showed that the negative attitudes of employees in the team are predictors of the deliberate counterproductive and subversive behavior of the employee, from absenteeism to various forms of revenge [11]. One of the most common and important issues in personnel security management associated with both internal and external risks is the problem of data leakage or insider risk. Frank L. Greitzer, Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, and Ryan E. Hohimer (2012) describe a model of employee behavior evaluation based on a set of 12 behavioral indicators for identifying those employees who have elevated insider risk (in other words, those who can harm the organization or its employees) [6]

The Bayesian model, the nonlinear model of the neural network with feedback (ANN) and the linear regression model, factors in which certain psychological indicators of a person are laid, that are conditionally available in each company, have been tested by the above-mentioned authors. As a result of the study, the Bayes model was chosen as the best in terms of stability, visibility and quality of predictions. The application of this model allows you to make forecasts of the probability of a threat to personnel security by each employee based on the analysis and combination of these behavioral factors. This research also emphasizes the need to use company data collection systems that can also record the psychological and behavioral performance of employees, to provide a comprehensive solution and the ability to implement the model previously described.

Thus, the authors of this model describe the possible architecture of the CHAMPION system, which provides a fair and consistent approach to monitoring the psychological characteristics and behavior of employees that benefits both employees and employers. Among the strengths of this model is the relative simplicity of given tasks implementation and ease of use. In addition, the Bayesian model is based on probabilities, so it can give predictions even in the absence of real observational data (for example, for new employees). Moreover, considering the characteristics of each employee helps to assess better the probability of a threat, so this model is more practical in many companies. To the weaknesses can be attributed the relative subjectivity of the assessment of behavioral factors from other employees of the company, which cannot always assess the presence or absence of certain characteristics from their colleague.

Another model of psychosocial approach is presented in the work of Sokolowski and Banks, which is based on the methodology of agent modeling [7]. According to the canons of this methodology, employees of the organization are considered as agents that interact with other employees and the organization in the environment. Each agent (employee) can be represented by the layout of three behavioral components: emotional, rational, and social. These three components are united, forming the general attitude of the agent to the situation and adopting a decision that is considered as a binary relation. This structure has been used to represent each employee (insider) as a person who may adversely affect the company's security at some point, or regular employee that poses no threat.

III. The Aim of the Article

The aim of the article is to provide arguments for the application of the Bayesian network in the modeling of risks and threats as components of a comprehensive human resources management system at the enterprise, using a psychosocial approach.

IV. Research Results

According to the psychosocial conceptual-methodical approach that integrates the psychological characteristics of a person and his behavior as an employee in the internal environment of the enterprise, the author of this article, based on the above-mentioned five-factor model and previous studies of the author [12], developed a model for diagnosing threats to personnel security of the enterprise. This model is based on the identification of specific features in the behavior of workers, which (aspects of behavior) serve as preconditions for the risk of personnel hazards. The scientific hypothesis of constructing a model is that the psychological state of employees' dissatisfaction and the manifestation of social deviations, both in the internal environment and beyond, becomes of paramount importance in the violation of personnel balance and the occurrence of real threats to human security.

To implement the proposed scientific hypothesis, an approach based on personnel data that will be available to the personnel department is used. The psychological indicators used in the model are given in Table. 1

TABLE I. CHARACTERISTICS OF INDICATORS FOR A PSYCHOSOCIAL MODEL

Indicator mark	Indicator	Characteristic
Ind1	Dissatisfaction	An employee shows dissatisfaction with the current situation. Appear chronic signs of discontent - strong negative feelings due to the fact that the employee did not receive promotion, results of his work was underestimated or wages were not increased.
Ind2	Feedback rejection	An employee hardly accepts criticism; he does not want to admit the mistakes; may try to conceal mistakes by lie or deception.
Ind3	Anger management problems	An employee often allows anger to accumulate inside; the worker has problems with preserving the emotional feelings of anger or fury. Holds strong insults.
Ind4	Separation/ disengagement	The worker is dismissed, closed and strives not to interact with individuals or groups, avoiding meetings.
Ind5	Disrespect to leadership	An employee ignores rules, authority or policies and feels above the rules.
Ind6	Low productiveness	The employee received remarks (oral warning, written reprimand, suspension from work) on the basis of unsatisfactory work.
Ind7	Stress	An employee experiences a physical, mental or emotional tension with which it is difficult to cope with.
Ind8	Confrontation	An employee is involved in hooliganism or intimidation or shows aggressive behavior
Ind9	Personal problems	An employee experiences difficulty with delineating personal problems from work problems that impede his work.
Ind10	Egocentrism	An employee ignores the needs or wishes of others, primarily related to their own interests and well-being.
Ind11	Unreability	An employee cannot fulfill his obligations / promises.
Ind12	Absenteeism	The employee is characterized by chronic unjustified absenteeism.

Source: compiled by the authors

It must be emphasized: each of these indicators has different effects on the estimated level of risk. For example, delineation and dissatisfaction are usually considered to be more influential factors than unreliability, to investigate the personnel threat and the possibility of counterproductive behavior of one or another employee.

We emphasize that judgments based on observations will necessarily be subjective, which may be one of the disadvantages of this model. However, personnel management with this model will be able to understand better the nature and indicators of potential threats to human security. The most important thing is this approach and this model that provides the Human Resources and Enterprise Security Department with a tool for prior warning of possible public office offenses committed by employees.

To implement the approach described above, the author of the article used the Bayesian network (BN), which is a relatively new direction, which appeared at the interface of probability theory and the theory of graphs. BN is graphs that have certain characteristics. The idea of introducing BN consists in presenting cause and effect relationships, common to the process, in the form of a graph. The construction of the model uses the Bayesian theorem, which associates the a priori and a posteriori probabilities of the causes after observing the consequences.

Psychosocial indicators and personnel hazards risk are realized in the form of binary variable nodes in the Bayesian model, as shown in Fig. 1. In particular, each indicator for each employee can be encoded by a binary variable, where 1 means the presence of an appropriate characteristic in the behavior of a particular employee, and 0 is its absence.

Fig. 1. Schematic model of the Bayesian network
Source: compiled by the authors

The development of the Bayesian network takes several steps. Firstly, a network of connected conditionally dependent random variables is constructed, each of which takes value from a certain set. In the model proposed by the author, these values are 0 and 1, depending on whether there was an indicator in the behavior of a particular employee. Secondly, a priori probabilities are assigned to each variable. These probabilities reflect the frequencies with which random variables take certain values.

The third step in the development of the Bayesian network is to determine the impact of indicators on the risk of personnel hazards. One way to do this is to consult with specialists of human resources department to enter numerical values directly into the probability table for each combination of indicators in the Bayesian network. It is clear that the use of estimates of small number of specialists of one organization, acting as experts, is associated with large number of complex judgments, which combines a different number of factors.

Since this methodological approach is not effective, the author uses another scenario of applying the Bayesian network. For estimation of conditional probabilities, the results of expert evaluations based on researches conducted in 10 organizations were used. Thus, a statistical sample of data was created for 24 people, where each employee was exposed from 1 to 5 previously identified indicators. Subsequently, 10 experts from the staff of various organizations identified risk indicators for each individual according to existing indicators in her behavior. Therefore, the total set was 240 observations. Moreover, each of the experts assessed the importance of indicators from the least significant to the most significant for determining the destructive and threatening behavior of this employee.

The statistical properties of the created database showed a rather high degree of coherence of opinion among experts regarding the importance of indicators. Quite interesting was the fact that the egocentrism index has the highest standard deviation among the estimates of all indicators, while absenteeism is the least standard deviation. The most dangerous indicator of personnel security was the dissatisfaction and disrespect for leadership as a result of expert estimates.

Minor standard deviations in estimates have been evidence of a sufficient, though not absolute, level of consensus on the situation of personnel security by each employee. In addition, the calculated Pearson correlation coefficients and Kendall's agreement for this dataset indicate a high level of consensus among experts.

At the same time, the lowest standard deviation is 6.77, and the highest is 27.33, which indicates that it is difficult for individual workers to evaluate clearly. This statistics also confirms the subjectiveness of expert assessments. Meanwhile, using the thoughts of 10 experts helps somehow averaging the results of assessments, which may be one way to reduce subjectivity.

The Bayesian network was tested by the author using a cyclic batching procedure, leaving 24 cases from one evaluator for testing, while 24 cases from each of the remaining nine experts were used to evaluate network parameters. In order to estimate it, the maximum credibility method was used to study the probability of risk. The modelling was carried out in the R Studio environment.

The Bayesian predictions for 240 remaining tests are shown in fig. 2. The scattering diagram indicates a clear vertical separation between predictions. Although expert assessments in these cases do not show this division explicitly, the Bayesian network allows us to derive this model from expert forecasts. In general, the determination coefficient R2 = 0.598 for the constructed linear regression of the dependence of model predictions and real data of experts' estimates testifies a sufficient level of significance.

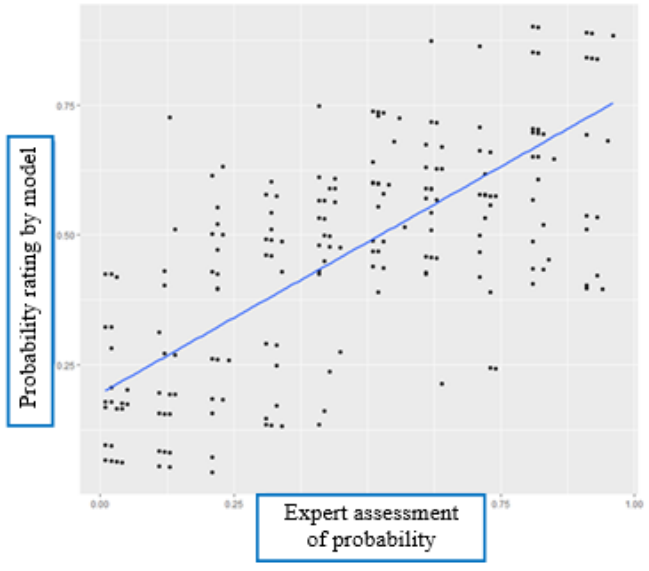

Fig. 2. Predicted possibility of risk according to the Bayes model.
Source: compiled by the authors.

After evaluating conditional risk probabilities, the Bayesian model can be used to predict the possibility of risk with regard to the impact of various employees on the personnel security of the enterprise. Yes, for the forecast, 12 test cases were used (see Table 2). As a result, a posteriori probabilities for each employee were obtained. Afterward, employees of the enterprise can be classified into 2 types - those who may cause threat to personnel security and those who cannot. The first type included those workers for whom the risk probability was estimated at more than 0.5.

TABLE II. TEST DATA FOR RISK PREDICTION

Co-worker	Ind 1	Ind 2	Ind 3	Ind 4	Ind 5	Ind 6	Ind 7	Ind 8	Ind 9	Ind 10	Ind 11	Ind 12
№1	0	0	0	1	0	0	0	0	1	1	0	0
№2	0	0	0	0	1	0	1	0	1	0	0	0
№3	0	0	0	0	0	0	0	0	0	0	0	0
№4	1	1	1	1	0	0	1	0	1	1	1	0
№5	0	0	0	0	0	0	0	0	0	0	0	0
№6	0	0	0	0	1	1	1	0	0	0	1	0
№7	0	0	0	0	0	0	0	0	0	0	0	0
№8	0	0	0	0	0	0	0	0	0	0	0	0
№9	0	0	0	0	0	0	0	0	0	0	0	0
№10	0	0	0	0	0	0	0	0	0	0	0	0
№11	1	1	1	1	1	0	1	0	1	1	0	0
№12	1	1	1	0	1	1	1	0	0	1	1	0

Source: compiled by the authors.

Aposterior probabilities are clearly shown in Fig. 3, have revealed that employees under numbers 4, 11, 12 can be sources of data leakage or other counterproductive behavior that endangers the company. Instead, workers 1, 2, 6, who are characterized by somewhat different indicators of psychology and behavior, do not pose a significant threat, as their characteristics do not form a sufficient level of risk.

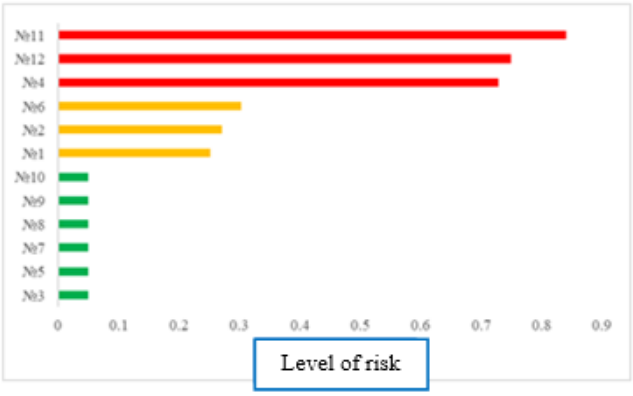

Fig. 3. Graphical representation of personnel risk assessment based on psychosocial model.
Source: compiled by the authors.

The Bayesian network, used in the development of this model, has two considerable advantages. Firstly, regression models and artificial neural networks usually require a complete set of data for each indicator, while the Bayesian network can be built on incomplete data and complemented by a priori probabilities. Secondly, in comparison with an artificial neural network, the Bayesian network is more acceptable and comprehensible to end-users as it provides a simpler explanation of the choice of parameters and modeling of personnel hazards risks. Furthermore, the "average" risk predictions generated by the model, represent the consolidated experience of experts which is better than predictions that may be provided by an individual expert due to possible data processing constraints, individual deviations,

or different experiences. This model also allows to diagnose employees automatically, regardless the experience and the state of the experts.

The following algorithm can be used to implement the above-mentioned approach to the assessment of personnel hazards risk at an enterprise:

1. To form a complex of psychosocial indicators for monitoring. This step should be implemented together with representatives of the human resources department with the involvement of psychologists.

2. Create an information system for continuous monitoring of changes in these indicators among employees. At this step, it is advisable to involve external psychologists and human resources specialists who will carry out the relevant tests as well as program engineers to create an aggregation application and analyze the data obtained.

3. Creating a software product to convert the values of certain indicators into the level of risk of a possible threat and counterproductive behavior of an employee. To do this, you can use open source algorithms and implement them on their own or through personnel outsourcing. However, this method takes a lot of time on implementation and the need to attract additional resources for continuous maintenance of the system's functional capabilities.

Another way to implement steps 2-3 is to purchase specialized software packages that already have the above-mentioned features combined (such as Midot and Exabeam).

4. Decision making based on the received risk data, carrying out preventive work, as well as a more detailed analysis of the peculiarities of the psychology and behavior of workers who have high risk of personnel hazards.

The given algorithm has a cyclic character, because psychosocial indicators used to identify the probability of threats to personnel security are being affected by a number of factors that determine their variation.

V. CONCLUSIONS

The results of the authors' research suggest that a comprehensive tool for identifying risks and threats in the company's personnel safety management system is a symbiosis of such key components as the objective diagnosis of psychological qualities and employees' motivation, which determines their behavior in the internal environment and beyond.

In the course of scientific research the following conclusions were made:

To predict the probability of personnel hazards, it is advisable to use the Bayesian network, which contains indicators that characterize the psychology and behavior of employees in the internal environment. The arguments for the success of applying such a methodical approach in the management of personnel security of an enterprise provide the possibility of using incomplete data supplemented by a priori probabilities, as well as its clearness for users regarding the choice of parameters and modeling results obtained.

The model, developed by the authors and presented in the article, allows carrying out psychosocial diagnostics of the employees regardless the level of qualification and sphere of experts competence. It can be introduced into the practice of assessing the psychosocial potential of employees, which will allow not only to identify threats to human security, but also to identify directions for improving the motivation mechanisms as a precondition for enhancing of personnel security.

The following steps should be taken in the formation of an enterprise personnel security system, in particular: creation of a complex psychological and technological system of information protection and reduction of insider threats risk; the transition to the world`s best samples of encryption information; creation of a system for monitoring employee activity based on computer network data and weekly reports with detailed analysis; development and implementation of a system for monitoring the psychological state of employees of the enterprise.

REFERENCES

[1] A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, "The "Big Picture" of Insider It Sabotage across U.S. Critical Infrastructures", *Insider Attack and Cyber Security*, Vol 39, pp. 17-52, 2008.

[2] R. Willison, and M. Warkentin, "Motivations for Employee Computer Crime: Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice", in *IFIP TC 8 International Workshop on Information Systems Security Research*, Copenhagen, Denmark, 2009, pp. 127-144.

[3] E. D. Shaw, and L. F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders. Report 1 - Overview and General Observations", Technical Rpt. TR 0504, Defense Personnel Security Research Center, Monterey, CA, Sep. 2005.

[4] L. A. Kramer, R. J. Heuer Jr., and K. S. Crawford, "Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage", Technical Rpt. TR 05-10, Defense Personnel Security Research Center, Monterey, CA, May 2005.

[5] M. Keeney et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", U.S. Secret Service and Carnegie-Mellon University, Software Engineering Institute, CERT Coordination Center. 2005.

[6] F. L. Greitzer, L. J. Kangas, C. F. Noonan, and A. C. Dalton, "Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats", in *45th Hawaii International Conference on System Sciences*, 2012, pp. 2392-2401.

[7] J. A. Sokolowski, and C. M. Banks, "Agent implementation for modeling insider threat", in *Winter Simulation Conference (WSC)*, Huntington Beach, CA, 2015, pp. 266-275.

[8] J. R. C. Nurse et al., "Understanding Insider Threat: A Framework for Characterising Attacks" in *IEEE Security and Privacy Workshops (SPW)*, 2014, pp. 214–228.

[9] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams" in *31st AAAI Conference on Artificial Intelligence*, San Francisco, California, 2017, [Online]. Available: https://pdfs.semanticscholar.org/8c1f/c5ba0b38ba5b71374f1fd7bc009ebf963af4.pdf?_ga=2.265412175.1999402385.1566822158-2103319545.1566822158. Accessed on: May 10, 2019.

[10] R. McCrae, and P. Costa "Big five personality factors" [Online]. Available: https://fc.vseosvita.ua/0010bc-73ae.pdf. Accessed on: May 12, 2019.

[11] M. Workman, "A Field Study of Corporate Employee Monitoring: Attitudes, Absenteeism, and the Moderating Influences of Procedural Justice Perceptions", *Information and Organization*, vol.19, pp. 218-232, 2009.

[12] D. Zatonatskiy, "Innovation Methods and Models of Personnel Security Management: Opportunities and Imperatives of Use at Ukrainian Enterprises", *Marketing and Management of Innovations*, vol. 1, pp. 294-301, 2019.