Marketing and Management of Innovations
Issue 1, 2019

ISSN 2227-6718 (on-line)
ISSN 2218-4511 (print)

UDC 331.1
http://doi.org/10.21272/mmi.2019.1-24

JEL Classification: J28, M50

Dmytro Zatonatskiy,
The National Institute for Strategic Studies, Ukraine

INNOVATION METHODS AND MODELS OF PERSONNEL SECURITY MANAGEMENT: OPPORTUNITIES AND IMPERATIVES OF USE AT UKRAINIAN ENTERPRISES

Abstract. *In the modern world, issues of personnel security management are getting more popular and significant in order to protect companies from internal and external threats. The article analyses modern approaches and models of personnel security management in the structure of economic security. The aim of the paper is to develop recommendations for the use of modern information systems and models of personnel security management for Ukrainian enterprises of strategic importance to the national economy. It is determined that the most general and broad approach to the definition of personnel security involves not only prevention of violations of the norms and principles of confidentiality of information by the personnel but also the organization of the security of the personnel itself, therefore, there is a need for the formation of an integrated system of personnel security management at the corporate level. The author's analysis of modern systems of personnel security management has shown the importance of researching the psychological and behavioural characteristics of employees not only in the corporate environment but also beyond its borders. It has been proved that the introduction of modern modelling techniques (in particular, the Bayesian model, the nonlinear model of the neural net with feedback, linear regression, k-mean algorithms, etc.) will contribute to the strengthening of the system in the practice of providing personal security under the influence of external and internal threats. It is recommended that domestic enterprises introduce a comprehensive and integrated personnel security system to improve the practice of psychological diagnosis and monitoring of employees' actions, in particular, improving the systems for collecting information on employee behavioural indicators in the corporate environment and beyond. The necessity of using the modern toolkit of the technical component of information security and certification system using the international standard ISO 27001 is proved, which significantly improves personnel security management in the structure of economic security of enterprises, reduces operational risk and increases the awareness of managers and ordinary employees. It is recommended to introduce improved technical systems in those types of activities and industries that are strategic for the economic growth of Ukraine's national economy and ensuring the country's defence and competitiveness.*

Keywords: personnel security, economic security, personnel security management, personnel security models, personnel management.

Introduction. The modern world, in which the economy and society develop, is undergoing considerable transformations of information and communication character. Everyone somehow becomes involved with innovative communication channels and information systems. The formation of a new (digital) economy and a post-industrial society, the deployment of the fourth industrial revolution simultaneously creates new opportunities and cause new threats. In such circumstances, one of the most pressing challenges is to ensure the confidentiality of information, which is becoming a strategic resource. The proliferation of social networks, the use of cloud technologies, the likelihood of access to large amounts of institutional and corporate data, have increased the risks of unauthorized use of personal data and corporate information. In the overwhelming majority of organizations, information security issues are given sufficient attention. However, it is important to realize today that technologies and tools for preventing the risks and threats of information security should become systematic and go beyond the formal control rules. The carrier and source of the dissemination of strategically important information have always been and remains a person, regardless of how perfect forms of accumulation and channels of information transmission. Set forth above shows that in the modern world issues of personnel security management are getting popular and significant in order to protect companies from internal and external threats.

Cite as: Zatonatskiy, D. (2019). Innovation Methods and Models of Personnel Security Management: Opportunities and Imperatives of Use at Ukrainian Enterprises. *Marketing and Management of Innovations*, 1, 294-301. http://doi.org/10.21272/mmi.2019.1-24

Literature Review. The theoretical foundations and practical aspects of personal security are the subjects of research by many domestic and foreign theorists and practitioners. Thus, in scientific publications of Puchkova S. (2013), modern approaches to personnel management for the preservation of personal security of the enterprise are analysed. In particular, attention is focused on the need for the use of information systems and technologies for obtaining objective information in the staff selection process; The advantages and disadvantages of the polygraph, Midot System, Extended DISC management system have been substantiated, which has allowed determining the range of tasks that can be solved using these personal technologies. In the study of Zhivko Z. (2013) the conceptual foundations of personnel security management as a subsystem of a comprehensive system of economic security are developed. In general, the concept itself is presented in the work and its elements are described, as well as a general algorithm for personnel security assurance at the enterprise. The synthesis of the scientific work has proven that in the scientific literature several approaches to the analysis of personnel security management at the enterprise have been formed. One group of researchers stresses the need to create information systems and data access control systems in such a way as to avoid the possibility of causing damage to the company by employees of the organization in order to provide effective personnel security. This approach is discussed in particular by Al-Dhahr et al., (2017), which addresses the question of the effectiveness of using international information security management systems as one of the ways to efficiently manage human security. Another group of researchers uses modern mathematical approaches and methods to model the impact of various factors on the possibility of leakage of data, mainly through the dissemination of confidential information by the company's staff. The work of Frank L. Greitzer et al. (2012), who applied and compared several of the algorithms of the landing date to study the insider risk problem, is fundamental in this area. As a result, the authors referred to the highest performance indicators of the Bayesian approach and presented the architecture of the CHAMPION personnel monitoring system for effective personnel security management. However, the current scientific basis for the development of perfect practical mechanisms for providing personal security does not meet the needs of the present. It should be acknowledged that in most of the available publications, personnel security issues are mostly fragmentary, there is a lack of systematic use of interdisciplinary research methodology.

The aim of the study is to develop recommendations for the use of modern information systems and models of personnel security management for Ukrainian enterprises of strategic importance to the national economy.

Results. Personnel security has been and remains the concept of complex and multifaceted, so domestic and foreign authors singled out different approaches to defining the concept and understanding of the essence and content of the interpretation of the category of «personal security». Personnel security occupies a dominant position with respect to other elements in the company's hierarchical security system, as it is tangent to the personnel, which today is recognized as the most valuable asset and strategic resource of enterprises. However, recognizing the priority of human resources, it is important to note that it is the staff that creates the preconditions for significant threats to the enterprise. Thus, one of the most common negative consequences of imperfect personnel security management is the leakage of information. According to a global study of leakage of confidential information held by the InfoWatch (2018) analytical centre, the amount of data leakage in the world in 2017 compared to 2016 increased by 37%, and their volume increased almost 4 times. In fig. 1. The visual format provides data on the increase of information leakage in the first half of 2018 compared to the first half of 2017. Confirmation of the information leakage phenomenon has become a series of high-profile cases related to access to the AADMAAR identification system in India, which contains biometric information of Indian citizens, and the use of Facebook's 87 million Facebook users in March 2018.

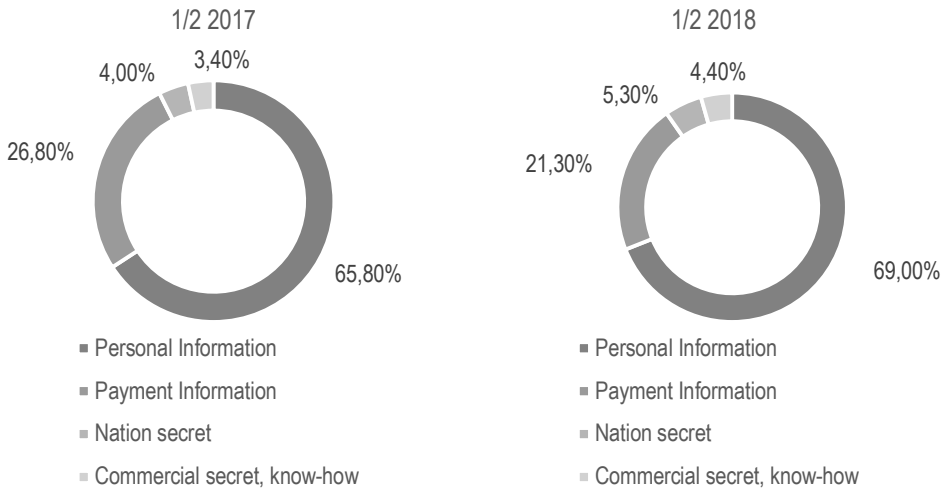

Figure 1. **Leakage distribution by data type, ½ 2017 – ½ 2018 y-oy**
Source: InfoWatch (2018).

The largest sources of data leakage were employees of companies (50.3%) and external fraudsters (41.7%). Personal data and billing information are the main type of data, the origins of which were greatest during 2017. Almost 70% of all leaks occurred through the network (browser), while the leakage from other sources did not exceed 10%. According to Juniper Research (2018), by 2019, cybercrime will cost businesses more than $ 2 trillion – four times more than in 2015, and the average cost of data leakage will exceed $ 150 million by 2020. The most common and broad approach to defining human security implies not only the prevention of violations of the rules and principles of the confidentiality of information by staff but also the organization of the security of the staff themselves. According to the author, on such a general rule, a complex system of personnel security management at the corporate level should be formed. One of the most up-to-date approaches to addressing the issue that has become the subject of research in the framework of the article proposed by potential readers is described in the Xiaojuan Ma (2016) study, which covers an integrated mobile security management system based on the object-oriented modelling method. The author suggests defining this system on the basis of log audit, event monitoring and password management in the company's corporate information network. The publication highlights the need for simulation of security events (data) management based on the comprehensive aggregation of logs from different sources. After collecting the required data, the author proposes to introduce a modified virus checking and prevention system in which passive protection is replaced with active. The author defines such protection as the most effective way of managing security in the information system of any company at the present stage. As a result, the proposed system should facilitate the comprehensive protection of personal data of employees and corporate information within the established network. Thus, the management of personal security in terms of preventing external threats, namely the possibility of virus entry into the system by outside employees of the company network and the commission of illegal actions.

At the same time, there is a narrower interpretation of personnel security. For example, O. Kirichenko (2008) defines human security as a legal and informational provision of the personnel management process, namely: resolving legal issues in labour relations, preparing regulatory documents that regulate them, and providing the necessary information to all personnel management units.

In this approach, in foreign literature, the management of personal security at the macro and micro levels is considered. In the article Li T. and Li L. (2015), a model of the combination of human resources and information and social security at the state level is proposed based on the development of a special computer system. Meanwhile, the system is based on the collection and processing of large volumes of data and state support through the introduction of special state institutions that should address the issues of social protection of human resources at enterprises and ensure the sustainable development of the personnel management system at the state level. Therefore, in Ukraine, it is also important to develop its own national strategy and personnel management system to ensure effective social security of citizens in the current economic and political situation in the country.

The study of Zykov S. (2001), who developed a problem-oriented model for integrated corporate resource management at the enterprise, is interesting in the questions of the micro-level aspects of personal security. The basis of the metadata model is the theory of categories, methods of finite sequences, and semantic networks. On the basis of such a model and data, the scheme for the creation of a corporate information management system for personnel management and its security is generalized. As a result of the practical implementation of this model at UniQue enterprise, significant reductions in terms and costs for implementation as well as increased portability, scalability and ergonomics compared to existing commercial systems of this kind, which enabled the effective management of personal security has been proved. At the present stage, more and more systems of this kind are created using cloud-based technologies. For example, Odun-Ayo I. et al. (2017) proposed an «OnibereOdunayoSecurity-4» security model (OOS-4) for a human resources information system using Google Cloud Platform. This personnel management system, unlike most existing developments, provides encryption of all data, from the recruitment process to its release, and provides a unique level of authorization that gives different rights to different categories of users. Thus, from the point of view of personnel security management, such systems bring a new level of information protection to detect and prevent threats directed at the staff and the intellectual potential of the company. Another approach to the definition of personal security is proposed by Chumarin I. (2005), which sees in the personnel security a process of prevention the negative impact on the company's economic security at the expense of risks and threats associated with staff, its intellectual potential and labour relations in general. Modern studies of personnel security management from this perspective are increasingly using fuzzy logic and multicriteria tasks, mostly focusing on the psychological characteristics of the employee.

The work of Astakhova L. (2015) investigated the influence of socio-technical factors and the modern humanitarian approach to assess the trust of employees in the information system. The author defines the term «reliability of the information system for personal security» and proposes a multi-criteria classification model of the levels of reliability of the information system of personnel security, which is based on the trustworthiness of employees to the organization, the level of mutual trust, monitoring of the cultural capital of the organization, the level of labor risks and the level of awareness of employees about information security. As a result, the author proposed to determine the level of reliability of personnel security in 7 levels, concerning the socio-cultural and humanitarian factors of the information system. In the present situation, many practitioners in the field of personnel security emphasize the importance of formalizing the management of personal security, stressing the need to develop special rules and regulations for personnel in order to prevent undesirable actions associated with causing the school's organization. Nowadays, the methods of providing and managing personnel security in foreign companies, in particular in Europe and the United States, are widely used, with the implementation of international standards for personal security and data access models for different categories of staff. Quite a lot of researchers point out the importance of introducing international quality standards for personnel security assessment. One of the examples of such a common standard for information security management at an enterprise can be ISO 27001. Al-Dhahri S., Al-Sarti M. and Abdul A. (2017) describe the use of information security

management models in an enterprise based on this international standard. Authors show that certification using this standard helps organizations to improve their asset management, in particular, its important component which is personal security. The article analyses the main areas of personal security with an emphasis on the management of each component. As a result, it has been shown that personnel management, in accordance with ISO 27001, provides a reduction in operational risk and increases awareness of managers and staff in the field of information security. In addition, the result of the study of these authors was a generalized sequence of actions for the implementation of the ISO 27001 information security management system in the company. Consequently, in order to create a reliable personal security system and its further development in the modern information world, Ukrainian enterprises should accelerate the certification of information security management based on the international ISO 27001 standard. On the other hand, many researchers point out the importance of creating an effective system for accessing data categories of people. A large number of control and data access control models, including the Clark-Wilson integrated model, the Harrison-Ruzzo-Ullman model, the Brewer-Nash model, and the Bell-LaPadula model, have been created for this purpose. Thus, in the study of Garnaut P and Thompson J. (2011), a comparison of the most common models of integration, control and data protection for use in the field of digital defence based on a definite number of criteria is given.

In recent years, management of security systems in the enterprise has been widespread, including those related to personnel, based on the methods of data mining. In particular, Zope A. R., Vidhate A., and Harale N. (2013) offer an overview of the various techniques of data mining for solving the problems of information security in the enterprise. The most commonly used implementations are firewalls that operate on the basis of set rules to protect the network against unauthorized access, and spam filtering systems and undesirable software applications in the letters, based on the simplest of which is the Bayesian rule. However, the most important in terms of personal security is the data leakage prevention systems that allow organizations to reduce the corporate risk of accidentally disclosing confidential information. The article analyses the model of the system's operation, based on one of the algorithms of the data mining, namely associative rules, for generation of warning messages and prevention of vulnerability of the system. The theory is proved, and practice has confirmed that one of the most common and important problems in personnel security management, which is related both to internal and external risks, is the problem of data leakage or the problem of insider risks. Frank L. Greitzer et al (2012) proposed a model for assessing employee behaviour based on psychological factors to identify those employees who are subject to increased insider risk (ie, those who can harm the organization or its employees). The authors tested the Bayesian model, the nonlinear model of the neural network with feedback (ANN) and linear regression, factors which set certain psychological characteristics of the person, the use of which is available in each company. The data collection and testing of the model was carried out by HR department experts. As a result of the study, the Bayes model was identified as the best in terms of stability, visibility and predictive quality. The analysis stresses the need to use the user data collection system, which can also record the psychological and behavioural characteristics of employees, to provide a comprehensive solution and the possibility of implementing the above model. So, the authors describe the possible architecture of a CHAMPION system that provides a fair and consistent approach to employee monitoring and benefits both employees and employers. Meanwhile, data collection using only the company's internal information system is not enough to comprehensively assess the data leakage risks. So, Alahmadi, BA, Legg, PA, and Nurse, JR (2015) have investigated how Internet activity (blogs, Twitter posts and Facebook profiles) can be used to predict the psychological characteristics of a person in order to identify potential insider threats. In the basis of this approach was put two components: 1) the correlation of personality characteristics (OCEAN – 5 essential personality traits) with the websites that this person visits, using categorical analysis of the text based on the LIWC dictionary; 2) insider threat model based on the k-medium method. Results of prediction of personality characteristics can be used to create a profile of

employees, on the basis of which various psychological studies can identify the risk of insider threats from employees. At the same time, such an approach may lead to conflicts as to legislative security and the moral aspect, since the collection of such data may be illegal and violate not only ethical principles but also legislative rules. Unlike researches based on the use of statistical models, there is an approach based on dynamic modelling of agent behaviour. Advantages of modelling the behaviour of agents consist of the method of representing a complex adaptive behaviour using the attributes of individual (heterogeneous) entities (agents) and the nature of their interaction in the system. Among the weaknesses of the simulation of the behaviour of agents is the high probability of inaccuracy in the compilation of behavioural equations, on which the behaviour of the whole system depends. In the paper Sokolowski J. and Banks C. (2015), an approach based on agent modelling using the structure of Epstein AgentAzero is highlighted. Agent_zero consists of three behavioural components: emotional, rational, and social. These three components are combined to ensure the general attitude of the agent to the situation and the adoption of 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 a non-threatened regular employee. The implementation of the Agent_zero emotional component is presented as the difference between the expectations of the insider and the fulfilment of these expectations as to its position in the company. Expectations of the insider vary depending on the initial, current and historical fulfilment of these expectations. Expectations in the model can be represented by the following equation (1):

$$E_{j+1} = \frac{F_1 p + \left(\left(\sum_{i=1}^{j} F_i\right)/j\right) c + F_j r}{p + c + r}, \quad (1)$$

where E_{j+1} – anticipation for the next modeling step, *F* – actual satisfaction at different times during modeling, *p* – the importance of primacy, in other words, how much attention employee pays to initial satisfaction, *c* – the importance of consistency, which shows the level that is given to average satisfaction over time, *r* – represents the employee`s emphasis on current satisfaction.

Then, the interpretation of the agent's satisfaction deficit is calculated using the following equation (2):

$$d_j = \left(E_j - F_j\right) a \quad (2)$$

where d_j – the difference in anticipation of satisfaction d during time j, concerning the interpretation of the insider, *a* – is the specific gravity specific for each agent.

The analysis of modern personnel management systems carried out by the author of this article showed the importance of researching the psychological and behavioural characteristics of employees not only in the corporate environment but also beyond its borders. One of the tools for implementing such a goal should be to monitor social networks and blogs. However, according to research results, the use of these models is rather limited. Thus, according to Watcher in 2017, only about 25% of Ukrainians had pages in the most popular Facebook network (Minchenko, 2018). Hypothetically, one can assume that the percentage of users of other social networks is even smaller, which prevents the desired information about all employees. The scale and pace of computerization, informatization and digitization in Ukraine, as well as the development of legislative norms in the field of data processing, provide grounds for determining the prospects for the introduction of models using information about employees, the source of which are social networks, which will be one of the effective tools for personal security in Ukraine.

Conclusions. The results of the author`s research provide grounds for asserting that the modern system of personal security of the enterprise, as an inherent component of economic security, is a

symbiosis of at least three elements – the perfection of technical solutions, objective diagnosis of psychological qualities of the individual and understanding of the motivation of employees.

The analysis of international experience has shown that the actual tools of a technical component of information security that closely correlates with personnel security are the certification system using the international standard ISO 27001, which significantly improves the management of personal security in the structure of economic security of enterprises, reduces operational risk and increases the awareness of managers and ordinary employees. Particularly important is the introduction of improved technical systems in those types of activities and sectors that are strategic for the economic growth of Ukraine`s national economy, the defence capabilities and competitiveness of the country.

There is no doubt that among the tools for providing personal security at the enterprise, issues of increasing the degree of technical protection of strategically important corporate information are actualized, but the primacy, according to the author`s deep conviction, belongs to the non-technical side. Therefore, for domestic enterprises, an important step in the implementation of an integrated and holistic system of personal security is the improvement of the practice of psychological diagnosis and monitoring of employees` actions, in particular, the improvement of systems for collecting information on employee behavioural indicators in the corporate environment and beyond. The introduction of modern modelling techniques (in particular, the Bayesian model, the nonlinear model of the neural network with feedback, linear regression, the k-mean algorithms, etc.) will contribute to the strengthening of systematicity in the practice of providing personal security under the influence of external and internal threats.

In the conditions of the formation of a new economy, when high-level information and communication technologies are developing rapidly, among the managerial aspects the issues of managing the psychological and motivational potential of employees are updated. Among moral values, a special place occupies trust, as a complex socially significant phenomenon of the reality of a modern, volatile and contradictory world, which has not yet received the proper scientific theoretical and applied rationale and is among the scientific interests of the author of this article. Among the issues of further scientific research by the author is the evaluation of the effectiveness of the application of various systems, methods and tools for personal security management at the enterprise.

References

Alahmadi, B. A., Legg, P. A., & Nurse, J. R. (2015). Using Internet Activity Profiling for Insider-threat Detection. *Proceedings of the 17th International Conference on Enterprise Information Systems*. Retrieved from http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220%2f0005480407090720.

Al-Dhahri, S., Al-Sarti, M. & Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications, 158*(7), 29-33.

Astakhova, L. (2015). Evaluation Assurance Levels for Human Resource Security of an Information System. *Procedia Engineering, 129*, 635-639.

Chumarin, I. (2005). Work with staff in the context of the overall security of the company. *HR management, 1,* 34–40.

Cybercrime will Cost Businesses Over $2 Trillion by 2019. *JuniperResearch.* Retrieved from https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Garnaut, P & Thompson, J. (2011). Review of Data Integrity Models in Multi-Level Security Environments. *DSTO Defence Science and Technology Organisation.* Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a542134.pdf

InfoWatch. (2017). Global research on confidential information leaks in 2017. Retrieved from https://www.infowatch.ru/report2017

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012). Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. *45th Hawaii International Conference on System Sciences*. Retrieved from https://www.researchgate.net/publication/261527163_Identifying_At-Risk_Employees_Modeling_Psychosocial_Precursors_of_Potential_Insider_Threats

Kyrychenko, O.A., Sidak, V.S. (2008). Problemy upravlinnia ekonomichnoiu bezpekoiu subiektiv hospodariuvannia: monohrafiia [Problems of management of economic safety of subjects of management: monograph]. Kiev: Universytet «Krok» [in Ukrainian].

Li, T., & Li, L. (2015). Application of Computer Technology in Human Resource Management and Social Security. *The Open Cybernetics & Systemics Journal, 9*(1), 1892-1897.

Minchenko, O. (2018). U Facebook vzhe 11 mln ukraintsiv [Facebook has 11 million Ukrainians]. *Watcher.* Retrieved from http://watcher.com.ua/2018/01/23/u-facebook-vzhe-11-mln-ukrayintsiv/

Odun-Ayo, I., Misra, S., Omoregbe, N., Onibere, E., Bulama, Y. & Damasevicius, R. (2017). Cloud-Based Security Driven Human Resource Management System. *IOS Press.* Retrieved from https://www.researchgate.net/publication/319037088_Cloud-Based_Security_Driven_Human_Resource_Management_System

Puchkova, S. I. (2013). Upravlinnia kadrovoiu bezpekoiu pidpryiemstva cherez suchasni kadrovi tekhnolohii [Management personnel security enterprise through modern HR technology]. *Naukovyi visnyk Odeskoho natsionalnoho ekonomichnoho universytetu – Scientific Bulletin of the Odessa National Economic University, 26 (205),* 43–54 [in Ukrainian].

Sokolowski, J. A., & Banks, C. M. (2015). Agent implementation for modeling insider threat. *Proceedings of the 2015 Winter Simulation Conference.* Retrieved from https://www.researchgate.net/publication/302479872_Agent_implementation_for_modeling_insider_threat

Xiaojuan, M. (2017). Research and Implementation of Computer Data Security Management System. *Procedia Engineering, 174,* 1371-1379.

Zhyvko Z. B. (2013). Kontseptualni osnovy upravlinnia kadrovoiu bezpekoiu pidpryiemstva [Conceptual bases of personnel security management of the enterprise]. *Zbirnyk naukovykh prats Tavriiskoho derzhavnoho ahrotekhnolohichnoho universytetu (ekonomichni nauky) – Collection of scientific works of Taurian state agrotechnological university (economic sciences), 2(1*), 103-111 [in Ukrainian].

Zope, A. R., Vidhate, A., & Harale, N. (2013). Data Mining Approach in Security Information and Event Management. *International Journal of Future Computer and Communication, 2,* 80-84.

Zykov, S. (2001). Towards Implementing an Enterprise Groupware-Integrated Human Resources Information System. Retrieved from https://www.researchgate.net/publication/2389488_Towards_Implementing_an_Enterprise_Groupware-Integrated_Human_Resources_Information_System

Д. А. Затонацький, *Національний інститут стратегічних досліджень (Україна).*

Інноваційні методи та моделі управління кадровою безпекою: можливості та імперативи використання на українських підприємствах

У сучасному світі для захисту діяльності компаній від внутрішніх та зовнішніх загроз все більшої популярності та значущості набувають питання управління кадровою безпекою. У статті аналізуються сучасні підходи та моделі управляння кадровою безпекою у структурі економічної безпеки. Мета статті полягає у розробленні рекомендацій щодо використання сучасних інформаційних систем та моделей управління кадровою безпекою для українських підприємств, які мають стратегічне значення для національної економіки. Визначено, що найбільш загальний та широкий підхід до визначення кадрової безпеки передбачає не лише попередження порушень норм та принципів конфіденційності інформації з боку персоналу, а й організацію захищеності самого персоналу, тому виникає потреба у формуванні комплексної системи управління кадровою безпекою на корпоративному рівні. Проведений автором аналіз сучасних систем управління кадровою безпекою засвідчив важливість дослідження психологічних та поведінкових характеристик працівників не лише в корпоративному середовищі, а й за його межами. Доведено, що посиленню системності у практиці забезпечення кадрової безпеки під впливом зовнішніх та внутрішніх загроз сприятиме запровадження сучасних методів моделювання (зокрема, байєсівська модель, нелінійна модель нейронної мережі зі зворотним зв'язком, лінійна регресія, алгоритми к-середніх та інші). Підприємствам рекомендовано запровадити комплексну та цілісну систему кадрової безпеки для поліпшення практики психологічної діагностики та моніторингу дій співробітників, зокрема – вдосконалення систем збору інформації щодо поведінкових індикаторів співробітників у корпоративному середовищі та за його межами. Доведено необхідність використання сучасного інструментарія технічної складової інформаційної безпеки, системи сертифікації з використанням міжнародного стандарту ISO 27001, що суттєво покращить управління кадровою безпекою в структурі економічної безпеки підприємств, зменшить операційний ризик та підвищить обізнаність менеджерів та рядових працівників. Рекомендовано запровадження досконалих систем технічного характеру в тих видах діяльності та галузях, які є стратегічними для економічного піднесення національної економіки та забезпечення обороноздатності і конкурентоздатності країни.

Ключові слова: кадрова безпека, економічна безпека, управління кадровою безпекою, моделі кадрової безпеки, управління персоналом.

Manuscript received: 10.01.2019.