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

MODERN METHODS OF PERSONNEL SECURITY MANAGEMENT AT THE ENTERPRISE UNDER THE INFLUENCE OF EXTERNAL AND INTERNAL THREATS

The world is rapidly undergoing massive digital transformation, where each person is connected in one way or another with the information environment, namely, the growth of the Internet and the role of social networks in human life, the active development of information systems and technologies. In society and business, more and more attention is paid to the confidentiality and integrity of information that is becoming one of the most important resources. Therefore, issues of personnel security management growing in popularity and significance in the world, to protect the company from internal and external threats.

Personnel security occupies a dominant position with respect to other elements of the company`s economic security, because it `works` with the personnel, which in any component is primary. However, when defining the primacy of employees in the organization`s activities, it is essential to note that significant threats to the company are caused by the staff. Thus, one of the most common negative consequences of mismanagement of personnel security is the data leakage. According to data leakage security report by the Analytical Center InfoWatch in 2017 compared with 2016, the number of data breaches in the world increased by 37 %, and their volume increased by almost 4 times [1]. The main providers of data leakage were their own employees (50.3%) and external fraudsters (41.7%). Personal data and payment information are the main type of data, leaks of which was the largest in 2017. Almost 70% of leak occurred through the network (browser), while the leak from other sources was no more than 10%.

Moreover, according to Juniper Research, the average cost of data leakage will exceed $ 150 million by 2020, and by 2019 cybercrime will cost business more than $ 2 trillion that is four times more than in 2015 [2].

The most widely used approach to the establishment of personnel security is not only to prevent the impact of personnel, but also to protect the personnel themselves. Under such circumstances, a comprehensive security management system in a particular company`s network must be formed. One of the most recent approaches to this issue is described in the Xiaojuan Ma (2016) investigation, which explores an integrated mobile security management system based on the object-oriented modeling method [3]. The author suggests defining this system on the basis of log audit, monitor development and password management in the company`s corporate network.

Quite a lot of researchers emphasize on the importance of introducing international quality standards for personnel security assessment. One of the examples of such an adopted standard of information security management system at an enterprise can be ISO27001. The paper of Al-Dhahri S., Al-Sarti M. and Abdul A. (2017) investigates the use of information security management models in an enterprise based on this international certificate [4]. Authors show that getting this certificate helps organizations better manage the security of their assets, in particular its important component-personnel security.

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. In the work of Frank L. Greitzer, Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, Ryan E. Hohimer (2012), a model for evaluating employee behavior based on psychological factors was developed to identify those workers with increased insider risk (i.e. those who can harm the organization or its employees) [5]. The authors tested the Bayesian model, the nonlinear model of the neural network with feedback (ANN) and the linear regression, factors that had certain psychological characteristics of a person, which are conditionally available in each company. The data collection and testing of the model was carried out with the help of HR department experts. As a result of the study, the Bayes model was chosen as the best in terms of stability, visibility and quality of projections. Furthermore, this work emphasizes the need to use user data collection systems that can also record the psychological and behavioral

performance of workers to provide a comprehensive solution and the possibility of implementing the model previously described. Consequently, 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.

The analysis of modern systems of personnel security management has shown the importance of researching employee data not only inside the company but also beyond its borders, including in various social networks and blogs. However, according to Watcher in 2017, about 25% of Ukrainians had pages on the most popular Facebook networks, the use of these models is very limited [6]. Nevertheless, in the future growth of computerization in Ukraine and enforcement of legislative regulations in the field of data processing, models using data from employees on social networks will become an effective tool of personnel security system in Ukraine.

Conclusions

Based on international experience, the necessity for Ukrainian enterprises to implement modern information security management systems ISO27001 and the newest models of data access systems from different groups of employees was substantiated. This will significantly improve the management of personnel security, reduce operational risk and increase the awareness of employees and managers. The priority sectors that require such changes are identified, namely, state-owned companies and the military sector.

Moreover, it is recommended for Ukrainian companies to improve employee monitoring systems, in particular further improving information gathering systems. On the basis of the analysis, it was determined that it is necessary to collect not only data from the use of computers and networks, but also the psychological states and characteristics of employees. Only on the basis of these data and modern methods of modeling (in particular, the Bayesian model, the nonlinear model of the neural network with feedback, linear regression, algorithms and others) will be able to provide effective management of personnel security at enterprises under the influence of external and internal threats.

References

1. InfoWatch. Retrieved from https://www.infowatch.ru/report2017
2. JuniperResearch. Retrieved from https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
3. Xiaojuan, M. (2017). Research and Implementation of Computer Data Security Management System. Procedia Engineering, 174, 1371-1379. doi:10.1016/j.proeng.2017.01.290 (Web of Science)
4. Al-Dhahri, S., Al-Sarti, M. & Abdul, A. (2017). Information Security Management System. International Journal of Computer Applications, 158(7), 29-33. doi:10.5120/ijca2017912851
5. 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. 2012 45th Hawaii International Conference on System Sciences. doi:10.1109/hicss.2012.309 (Scopus)
6. Watcher. Retrieved from http://watcher.com.ua/2018/01/23/u-facebook-vzhe-11-mln-ukrayintsiv/