European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.08.02.102

PEHPP 2019
Pedagogical Education: History, Present Time, Perspectives

THE PEDAGOGICAL APPROACH TO THE DEVELOPMENT OF INFORMATION SECURITY CULTURE

A.Vl. Vilkova (a), Vl. M. Litvishkov (b), B. An. Shvyrev (c)*
*Corresponding author

(a) Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia, mavlad67@mail.ru
(b) Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia, mavlad67@mail.ru
(c) Research Institute of the Federal Penitentiary Service of Russia, Moscow, Russia, bor2275@yandex.ru

Abstract

An enterprise is a set of employees and employees of different positions and responsibilities united by an interest in the result of the main business process in an atmosphere of service and corporate principles of communication and interaction part of which is the culture of information security, which is a collective awareness and respect for information security by all personnel. The urgency and relevance of the concept of information security culture in a modern technological society is noted. The authors test the hypothesis about the possibility of changing a person's behavior and developing a culture of information security during training in continuing education courses in the field of information security. All employees of the organization participate in the review regardless of their involvement directly in the technological process of information processing. An analysis of the results conducted by the authors made it possible to determine that training the organization's employees in the field of "information security" guarantees an increase in the average level of competence in information security issues and helps to develop a culture of information security. The development of an information security culture is based at least on an average level of literacy in information security issues. One of the priority points identified in the study is the influence of employees demonstrating high qualifications in information security issues on the training of their colleagues directly in their working places and inculcating an information security culture.

Keywords: Information security culture, advanced training, education, information security, training in working groups, continuous learning.

https://doi.org/10.15405/epsbs.2020.08.02.102
Corresponding Author: B. An. Shvyrev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Culture in itself is a welcome element of any process or phenomenon in the social environment. Due to the transition of the concepts of processing and protecting information from only technical and mathematical aspects to the plane of socially significant manifestations and, in general, the social significance of information and the safety of this information, information security demonstrates the need to inherit all the social elements of interaction, in particular the formation of a culture of handling it.

At present, quite often they talk about the importance of "creating a security culture". The idea itself is very important and topical, but quite difficult to put into practice (Lejaka, Veiga, & Loock, 2019).

The culture of information security can be a collective awareness and respect for information security by all employees of the enterprise (Gangire, Veiga, & Herselman, 2019). An enterprise is a set of employees and employees of different positions and responsibilities United by an interest in the result of the main business process in an atmosphere of official and corporate principles of communication and interaction, which is part of the culture of information security. Employees involved in information processes view the culture of information security as "the way everyone does it here." There is a subconscious perception by employees of information security in the work process and daily life. Information security in an organization with a developed security culture is an integral part of all business processes of the organization, innovative projects and service interaction. The goal of developing a culture of information security is a basic level of awareness of absolutely all employees of the enterprise.

Cultures exist on different scales, from families, soccer teams, to corporations and countries. The culture of small groups is usually based on local interests or a community of united individuals. In a global sense, culture is based on natural, global, human values and ancestral heritage due to the great diversity of individuals that are united. The phenomenon of culture demonstrates the impossibility of its creation and management by the will of one person, it is created by society on the basis of the meaning, texts and information that society owns. There may be cases when an information culture is formed on the basis of a corporate culture, and the presence of enthusiasm and motivation allows you to speed up its formation (Da Veiga & Eloff, 2010).

2. Problem Statement

The analysis of the orientation and content of information training of university students as the main means of forming the foundation of information culture is carried out in the works of Polyakov V. P. (Polyakov, 2006, 2016). The issues of full-fledged informational training of students with a high level of informational culture in a multi-level system of national education are considered in the works of domestic scientists (Astakhova, 2018; Ganieva, 2015; Gendina, 2009; Kozlov & Undozerova, 2017, 2018; Kuzina, 2016; Pirogov & Zavalnev, 2014; Undozerova, 2018). There is educational literature aimed at creating an information culture among students in higher education institutions (Fundamentals of information culture: an Electronic textbook of Scientific and technical information center of the Moscow state University, 2014; Formation of information culture of library users: methodological guide, 2010). In these works, the pedagogical aspects of studying information security and the formation of a culture of information security among students in various specialties of higher education institutions are considered. However, most

https://doi.org/10.15405/epsbs.2020.08.02.102
Corresponding Author: B. An. Shvyrev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

authors consider the concept of "information culture" in the sense of an information security culture, confining itself only to the security issues of information systems and resources, although information culture is a much broader concept. The digitalization of all life processes, both domestic and professional, imposes requirements on the level of awareness in matters of information security for all capable citizens of the country. The development of the necessary foundations of information security and the formation of a culture of information security for such an audience is an urgent task. To solve this, additional professional education courses of various levels are created and developed.

Veiga (2019) from the University of South Africa dedicated her research to measuring the level of information security culture. Heyden (2013) examines the importance of staff training on information security and solutions to raising awareness. The importance of developing a culture of information security and its impact on managing the organization's security is analysed in (Van Niekerk & Von Solms, 2010). The greatest result from continuing education courses is possible with optimal adaptation to the initial level of training of the audience. The following works are dedicated to assessing the existing culture of information security among employees of the organization (Alhogail & Mirza, 2014; Furnell & Thomson, 2009; Ngo, Zhou, & Warren, 2005; Schlienger & Teufel, 2003; Sherif, Furnell, & Clarke, 2015). The estimates obtained contribute to the development of the correct pedagogical approach to the formation of a culture of information security in the organization. These literary sources contain material on how to assess the culture of information security and specific techniques for conducting awareness-raising courses. At the same time, unlike students of higher educational institutions, the audience of students in continuing education courses has a number of differences. It is heterogeneous in age, education, professional activities and work responsibilities. All these factors must be taken into account when choosing pedagogical approaches and methods for developing the foundations of a culture of information security. Thus, the urgent task is to assess and analyze the culture of information security among employees of the organization who have been trained in continuing education courses in the field of information security.

3. Research Questions

How to evaluate the process of knowledge assimilation and training of employees of the organization in the courses of additional professional training to raise awareness on information security?

4. Purpose of the Study

The effectiveness of the pedagogical process of developing a culture of information security among students taking additional professional training.

5. Research Methods

When writing this paper, we used the results obtained by scientists on the issues discussed, together with the results of the research and teaching experience of the authors. The main research methods were theoretical (study and analysis of the Federal State Educational Standard in the direction of training 10.00.00 - Information Security (development of continuing education programs); and empirical - observation, survey, statistical analysis.

https://doi.org/10.15405/epsbs.2020.08.02.102
Corresponding Author: B. An. Shvyrev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6. Findings

Let us consider the results of training employees of various state and commercial organizations in continuing education courses in the field of “information security”, conducted for several years at Krasnodar State Technological University. A specific feature of this observation is that all employees in each organization took the training, without exception, in accordance with their professional tasks and the job duties performed.

Some of the trained employees demonstrated excellent results in mastering the material, most of the audience consistently mastered the material in accordance with the developed training program, and some of the lagging ones resisted, sabotaged and even tried to oppose the training. This ratio of employees is typical for training in most large organizations, and it corresponds to normal distribution law of a random variable graphically expressed as a Gaussian curve. This curve is bell-shaped, with a single maximum and symmetric about the ordinate axis and rapidly decreasing values with distance from the maximum.

The maximum dependency obtained corresponds to 75±5% of the total number of employees in the organization. This is the majority of employees who regularly attended classes and made an effort to study the material. They are consciously involved in shaping the organization's information security culture. However, the motivation for such training is usually not related to the desire to acquire new knowledge, but is due to administrative and disciplinary actions. The greater stimulating effect is marked not so much by motivation, but by a clear definition of the requirements of the job descriptions of both the position held and the higher one.

This approach, having the largest number of employees, at the same time shows very satisfactory results of training and subsequent application in professional activities, which demonstrates the importance of pedagogical aspects of employee training.

Employees, who make up about 10±3% of the entire audience, do not show a desire to learn, demonstrate a negative attitude to the educational process. Employees with low academic performance did not demonstrate diligence, concentration, or attempt to remember information. This behavior can be caused by low intellectual abilities of students, high workload at work, and lack of time and desire to learn. Employees with low results resent being forced to attend professional development programs and sabotage them passively or actively, do not attend training sessions or demonstrate and Express their denial of training and try to form a negative attitude among employees to educational programs.

Employees who demonstrate leading results make up about 12 ± 5% of the entire student audience and sincerely seek to learn as much as possible about information security. They attend classes with interest and look forward to training in the following programs and areas of information security. They may even strive to take an active part in the planning and organization of professional development events in the field of information security, take the initiative on issues of interest. These are precisely those people who can be used as translators of knowledge and training directly at the production site in working groups throughout the organization on issues of information security and inculcating a culture of information security. Thus, employee training is implemented in various ways.

Surveys of students by the significance of the knowledge gained immediately after training show multidirectional statistics, which are mainly determined by the personal and value orientations of the studied groups, but at the same time, positive dynamics of the significance of the training in professional

https://doi.org/10.15405/epsbs.2020.08.02.102
Corresponding Author: B. An. Shvyrev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

activity is clearly revealed by repeated testing. Such a clear dependence is caused regardless of the personal attitude to the courses, the assimilation of knowledge and their subsequent application in practice. In this situation, the person who receives knowledge goes to a different level of perception of situations that arise in professional activity. He applies knowledge on information security consciously and does not divide it into those that were obtained earlier in the courses and those that he acquired as a result of subsequent practical professional activity. Such dependence shows the importance of information security training for the formation of information security culture (Veiga, Martins, & Eloff, 2007). Studies have been conducted for several years at various advanced training courses in the field of "Information Security".

The analyzed dependence is an approximation of discrete values obtained as a result of observing the behavior of students. In fact, it was obtained by summarizing a large data array and in a particular case can have an excellent value, caused not only by the features of mathematical processing, but also by the target group undergoing analysis. The paper presents a general approach to the consideration of possible situations, which shows the most important thing - it is a stable growth of knowledge among employees after training. As a result, we can hope for the development of a culture of information security that employees will carry home after performing their duties and will show it in everyday life, at home.

The distortion of the curve in a particular case can be caused by the professional characteristics of the trainees. For example, it is obvious that the military is most likely interested in security and is inclined to unquestioningly follow orders, so the curve of the army unit can be significantly biased towards highly motivated employees. The maximum value of the curve determines the relative number of employees involved in training, in the case of incomplete coverage of staff, it may decrease. Some topics of information security can cause difficulties in studying and applying them at work. People with a liberal arts education most often have difficulty mastering the basics of security, while properly implementing the concepts they have learned. Not only with a humanitarian, but also with a technical education, employees may have difficulty adapting to new sophisticated modern technologies, which shows the need for continuous training and the inability to be an expert in everything.

7. Conclusion

The programs of the courses in the direction of "Information Security" should correspond to the current level of development of information tools and the needs of society. When choosing pedagogical teaching methods, find a compromise between the refinement of technical concepts and the generalization of information to a global level that is not practical in practice. An important point is the formation of the correct glossary of terms especially for employees receiving initial training. The use of slang forms and established expressions is advisable when upgrading the skills of experienced and competent employees, this approach will create a friendly atmosphere.

Training the organization's employees in the field of "information security" is guaranteed to lead to an increase in the average level of awareness of information security issues in professional activities and, as a result, contributes to the development of a culture of information security.

The formation of a culture of information security is facilitated by at least basic knowledge of information security among employees and the desire of management to develop.

One of the priority points identified in the study is the influence of employees who demonstrate high qualifications in information security issues on the training of their colleagues directly in the workplace, in working groups and in the promotion of an information security culture. Small-group training in production is very effective and does not require large financial costs.

Acknowledgments

We express our deep gratitude to the Department of Computer Technology and Information Security of the Krasnodar State Technological University and personally to the head of the department, Associate Professor A.V. Vlasenko for the assistance in conducting the research.

References

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology, 64,* 540–549.

Astakhova, L. V. (2018). Development of students trust culture in the context of information security. *Bulletin of the South Ural State University. Series: Education. Pedagogical Science, 10*(1), 63-70. [in Russ.]

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computer and Security, 29*(2), 196–207.

Ganieva, L. F. (2015). Formation of information security culture among university students. *Modern Trends in the Development of Science and Technology, 2-4,* 95-98. [in Russ.]

Formation of Information Culture of Library Users: Methodological Guide. (2010). Orel: Publisher Alexander Vorobyov. [in Russ.]

Fundamentals of Information Culture: Electronic Textbook of Scientific and Technical Information Center of the Moscow State University. (2014). Retrieved from https://imo.msun.ru/div/subdiv/ntic/books/book1/4.htm [in Russ.]

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: recognising the varying user acceptance of IT security *Computer Fraud & Security, 2*, 5-10. https://doi.org/10.1016/s1361-3723(09)70019-3

Gangire, Y., Veiga, A., & Herselman, M. (2019). A conceptual model of information security compliant behaviour based on the self-determination theory. *Computer Science*, 1-6. https://doi.org/10.1109/ICTAS.2019.8703629

Gendina, N. I. (2009). Information culture, creativity and creativity of a graduate of a higher school in the context of problems of human capital development of the information society. Part 2. *Information Society, 1,* 57-63.

Heyden, L. (2013). Information Security and Comprehensive Internet. *Avtomatizatsiya I Sovremennyie Tehnologii* (Electron. J.), *11,* 29–31. Retrieved from https://www.cisco.com/c/ru_ua/about/press/2013/05292013g.html

Kozlov, O. A., & Undozerova, A. N. (2017). Information culture of the individual in the context of the development of modern information society. *Man and Education, 4*(53), 46-52.

Kozlov, O. A., & Undozerova, A. N. (2018). Pedagogical conditions of formation of information culture of cadets of engineering specialties. *Man and Education, 3*(56), 123 – 131.

Kuzina, N. N. (2016). Methodological bases of formation of information security culture among students of pedagogical University. *Problems of Modern Pedagogical Education, 53*(10), 80-87 [in Russ.]

Lejaka, T., Veiga, A., & Loock, M. (2019). Cyber Security Awareness for Small, Medium and Micro Enterprises (SMMEs) in South Africa, 1-6. https://doi.org/10.1109/ICTAS.2019.8703609

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change. In: AISM (pp. 67–73). Australia, Perth.

Pirogov, A. I., & Zavalnev, V. I. (2014). Information culture as a resource for ensuring personal security in the information society. *Economic and Social-humanitarian Research, 2*(2), 123 - 128 [in Russ.]

Polyakov, V. P. (2006). Development of information security culture in higher education. *Acmeology, 4,* 87-90. [in Russ.]

Polyakov, V. P. (2016). *Aspects of information security in information training*. Moscow: Institute of Education Management of RAE. [in Russ.]

Schlienger, T., & Teufel, S. (2003). Information security culture: from analysis to change. *South African Computer Journal, 31,* 46–52.

Sherif, E., Furnell, S., & Clarke, N. (2015). *An identification of variables influencing the establishment of information security culture, 9*1, 90. https://doi.org/10.1007/978-3-319-20376-8_39

Undozerova, A. N. (2018). Theoretical and methodological approaches to the formation of information culture of cadets of military engineering specialties. *Hospitable Petersburg, International Thematic Electronic Conference, April 2018-access.* Retrieved from https://mcito.ru/publishing/teleconf/spig_4/submitted.html [in Russ.]

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: a management perspective. *Computer and Security, 29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Veiga, A. (2019). *Achieving a Security Culture.* Retrieved from https://doi.org/10.4018/978-1-5225-7847-5.ch005

Veiga, A., & Martins, N., & Eloff, J. (2007). Information security culture validation of an assessment instrument. *Southern African Business Review, 11,* 146-166.