THE MOTIVATION OF HIGH SCHOOL TEACHERS IN THE FORMATION OF THEIR OWN COMPETENCIES IN THE FIELD OF INFORMATION SECURITY

Student Polushkin D.P., Undergraduate Trejbach E.L., PhD Chernova E.V.,
Postgraduate Dokolin A.S.
Nosov Magnitogorsk State Technical University – Magnitogorsk city, Russia Federation
E-mail: denis@itmaster.su, hellenachernova@mail.ru, etreibach@yandex.ru, a.dokolin@gmail.com

Abstract: *The article describes the problem of involving high school teachers in establishing the national information security by applying their own competencies in the field of information security and protection in the educational process, the demonstration of their trainees and active implementation in their own professional activities. Tasks of the personal and proprietary information protection often not resolved, which is a potential threat to the learning process, research activities of the University, and can be used cyber criminals for cyber extremist or terrorist crimes. The teaching staff motivation is a cornerstone in forming the own competencies in the field of information security process. The traditional leadership approach to formation procedure of information security in this case is insufficient, as the teacher is a leader of a new person preparation, ready to operate successfully in an information society.*
KEYWORDS*: INFORMATION SECURITY, NATIONAL SECURITY, EDUCATION, PROTECTION OF INFORMATION, MOTIVATION, PROTECTION OF INFORMATION, THE TEACHER, COMPETENCE*

1. Foreword

In the framework of the Russian Federation information security modern doctrine, updated in 2016, as one of the state security threats voiced the problem of "low citizens' awareness in matters of ensuring personal information security" [1]. Today the specialists categorically state that cybercrime is out of control: in 2016 more than 2 billion user accounts were destroyed or stolen. During his address to the Federal security service of Russia, President Vladimir Putin announced that the number of cyberattacks on state information resources in 2016 compared to 2015 increased in 3 times. According to German Klimenko, the adviser of the Russian Federation President, "the most important trend today in that area is cybersecurity" [2]. Analytical activity of the state structures shows that the "measures to ensure the information security of the infrastructure, <...> with using the domestic information technologies and products often have no comprehensive framework" [1]. The development process of all spheres of human activity Informatization causes emergence of the individual and society information security problems [3].

Lack of understanding that need to start information security with yourself – that's one of the major individual, society and the state threat. Often, we hear that in the data breach blame the government, paying insufficient attention to the needs of citizens and society, however, upon closer inspection act, it appears that the fault almost entirely lies either on the staff or on the management, virtually non-competent in providing both personal and organizational security. Citizens mistakenly believe that they are too "small fry" in order to motivate highly organized hacker groups or petty cyber criminals. But, let's look at an episode of malicious activity on the example of quite a common banking Trojan "Dear Wolf". He gets on the user's computer when clicking on the last link in a phishing special letter and waits a user logs into your Bank account. After that criminals have access to confidential information of the victim and opportunity to steal money. As usual, the user may be attractive in the role of pawns – computer "botnet" – a network for DDOS attacks. The examples are innumerable.

2. Prerequisites and means for solving the problems

The intensification of cybercriminals of all kinds and categories, found that the network provides endless possibilities for the implementation of any criminal plans, from simple bullying, to direct threats to the state – clearly signals the need for urgent action on education and training citizens of the state, ready at least to avoid cyberattacks of any form, and, as a maximum – to prevent criminal activity online. And the leading role in the solution of this problem must belong to the universities which train future managers and engineers, and humanities – teachers and educators. The identity of the University teacher is often crucial in the development of a student's future profession. For example, the teacher can form a stable competence in the field of personal data protection and information security, even if the subject taught is not affiliated directly with these questions and doesn't aim to foster these competencies.

In practice, high school teachers rarely pay attention to the protection of personal information – phone numbers, home address, usernames, passwords from workstations, and more is not the information for them that needs to be closed. Storage of scientific data, information about objects, theses and dissertations, service information can be easily extracted and used for any interests. As an example, can be called a workflow element as a "draft" - reprint on already used documents. Privacy is violated more than full. We believe that a teacher should be motivated to form competencies in information security by oneself, and, especially, actively use and accentuation of these points when communicating with students.

3. The solution of the problem

It is possible to formulate the core competencies in the field of information security needed by the teacher for successful professional activity:

– protection of personal information, in the workplace, and in public access (social networks, Internet sites);

– protection of professional information;

– protecting students from inaccurate information;

– formation of critical thinking (of students and teachers) [4];

– application of standard and additional security in the workplace, mobile devices and network;

The main issue is the irresponsibility of the teacher, the unwillingness to use both in everyday and professional life the basic rules of information security and information protection. Thus, the employer raises the issue of incentives and motivation the employees on the formation of the required competencies.

4. Results and discussion

The problem of motivation and stimulation of the university faculty related to problems of implementation the management functions. The faculty is a key element of the higher school qualification of the teacher, his pedagogical competence, qualities, the General culture depends on the quality of training and the performance of all economic activity in the country. Hence, one of the most important directions of the University management is improving the system of scientific-pedagogical personnel motivation and stimulation. Studies have shown that the motivation of the teacher increases when he knows that his work is relevant to society. In his writings E. P. Ilyin said that "even a small sign of your attention to the needs of the people increases the commitment in the activity" [5].

M. H. Meskon, M. Albert, F. Hedouri, summarizing the view of many scholars say about "the existence of the four management functions, one of them is motivation, which is directly connected with the staff of the company and in the context of information security management does not lose its significance and status" [6]. In fact, the user often struggles with the problems of ensuring information security by the strengthening of control, all restrictions, prohibitions, punishments, etc. It requires a lot of

resources, inconvenience, leads to hostility. But in most cases, you can simply try to teach employees the safe work procedure (of course, you need to first make it simple, effective and straightforward), modify their behavior, to make them understand that it is in their interest. In fact, it will be a real fight with the source of the problem, not its consequences. And sometimes it is not as difficult as it seems, though unusual.

According to statistics, more than half of the losses that are suffered by the company due to incidents in the field of information security caused by the actions of the staff. And mostly they do not happen because of malice, but simply due to the low level of awareness of users. Thus, by teaching their employees basic rules in the field of information security, the company can significantly reduce the risk of security breach. Not for nothing, staff training is one of the main requirements of the international standard for information security management ISO/IEC 27001.

Statistics "studies of confidential information leaks in 2015" conducted by "InfoWatch", saying that in 54% of cases the perpetrators of the leaks were employees of the organization [7]. The same statistics research "InfoWatch" on this issue, in 2014 was 58% and in 2013 – 62% [8, 9]. Analyzing given statistics, we can say that now the amount of leakage through the fault of the employee is reduced, however, this trend is not apparent.

5. Conclusion

In our opinion, an effective solution to this problem is a close examination of the motivation theory of employees professional activity, which is essentially a way of raising attention to the issue of information security [10]. In General, it should be noted that the role of professorial-teaching staff in the formation of personality, ready to ensure their own information security is not yet sufficiently appreciated, and we believe that the work in this direction should be continued.

6. References

1. The information security doctrine of the Russian Federation: [05.12.2016 (Approved by the decree of the President of the Russian Federation 05.12.2016 No. 646)]. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (Accessed: 21.02.2017) (in Russian).

2. Spiridonov Maxim Runitology: Herman Klimenko, the adviser of the Russian Federation President. Available at: https://runetologia.podfm.ru/977 (Accessed: 17.02.2017) (in Russian).

3. Chernova E.V. Informatsionnaia bezopasnost' lichnosti i obshchestva: uchebnoe posobie [Information security of the individual and society: study guide]. Magnitogorsk, Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G.I. Nosova, 2017, 275 p. (in Russian).

4. Zerkina E.V., Chusavitina G.N. ICT: innovation unsafe // Narodnoe obrazovanie [National education], 2008, no 8, pp. 273 -276 (in Russian).

5. Il'in E.P., Balashov E.P. Motivatsiia i motivy [Motivation and motives]. St. Petersburg, Piter, 2000, 512 p. (in Russian).

6. Meskon M.Kh., Al'bert M., Khedouri F. Osnovy menedzhmenta: Per. s angl. [Fundamentals of management: translated from English]. – Moscow, Vil'iams, 2007, 702 p. (in Russian).

7. Investigation of confidential information leaks in 2015 the analytical center "InfoWatch" [Site of "InfoWatch"]. Available at: http://www.infowatch.ru/report2015 (Accessed: 15.02.2017) (in Russian).

8. Investigation of confidential information leaks in 2014 the analytical center "InfoWatch" [Site of "InfoWatch"]. Available at: http://www.infowatch.ru/report2014 (Accessed: 12.02.2017) (in Russian).

9. Investigation of confidential information leaks in 2013 the analytical center "InfoWatch" [Site of "InfoWatch]. Available at: http://www.infowatch.ru/report2013 (Accessed: 10.02.2017) (in Russian).

10. Talalai M.A. Motivation as one of the ways to increase productivity. Sovremennye naukoemkie tekhnologii [modern high technologies], 2014, no 7–1, 90 p. (in Russian).