Analysis of the Level of Training in the Basics of Information Security of Students of Zhetysu University named after I. Zhansugurov

Laura A. Smagulova[a], Shynar M. Asylbekova[b] and Nabira S. Yermekova[c]

Zhetysu university named after I. Zhansugurov, Zhansugurova st., 187a, Taldykorgan, Kazakhstan

Keywords: Information Technology, Information Security, Information Security, Education, Educational Program, Questionnaire.

Abstract: Trends in the development of the world community indicate an increase in the need for specialists who master the latest techniques in information and communication technologies, who have a high information culture and who are able to apply their knowledge and skills to ensure information security in their professional activities. The tasks of increasing literacy in the use of information and communication technologies, the use of standard methods of protecting information when working on a personal computer, in local and global networks, remain relevant. Therefore, the training of students in the field of information security and information protection needs significant improvement and development. The article is devoted to the analysis of the orientation and content of information training of students in the basics of information security in Zhetysu Univeristy named after Zhansugurov. The article reflects the results of the study, during which the learning outcomes of the EP were considered and a questionnaire was conducted among students to determine the level of training in the field of information security. Based on the results of the research, ways of solving the identified shortcomings and gaps in the university program are suggested.

1 INTRODUCTION

In connection with the development of information technologies and the computerization of all spheres of human activity, information security is becoming one of the most important issues in the company's activities.

Information security in the field of informatization refers to the state of protection of electronic information resources, information systems and information and communication infrastructure from external and internal threats (Law of the Republic of Kazakhstan).

Information is one of the most valuable and important assets of any business and must be properly protected. With the development of information communications, the possibility of damaging information that is stored and transmitted with their help arises at the proportional level, thus making the problem of information security of existing systems for storing, transmitting and processing information

vitally important for society (Melnikov, Kleimenov and Petrakov, 2012). Trends in the development of the world community indicate an increase in the need for specialists who master the latest trends in information and communication technologies, who have a high information culture and who are able to apply knowledge and skills to ensure information security in their professional activities.

In particular, the training of personnel in the field of information security and information technology is still relevant, providing not only the training of qualified specialists in the field of information security and information protection, but also the study of information security by all other categories of specialists trained under the vocational education system (Polyakov, 2006).

The market lacks specialists in the field of information security, information protection and cyber security. According to the Director of the Department of Employment of the Population and Development of the Labor Market of the Ministry of

127

Labor and Social Protection of the Population of the Republic of Kazakhstan, Baltabay Kappasov of MIA Kazinform: the demand for analysts in the field of information security will increase by 18% in 2024 when compared to 2017.

Currently, as noted by the director of the Research Institute of Information Security and Cryptology of the Eurasian National University named after L.N. Gumilyov Seitkulov E, the annual economic damage from unprofessional use and malicious impact on computer systems amounts to hundreds of billions of dollars (Seitkulov, 2016).

Based on all of the above, it can be stated that the problem of training personnel in the field of information security and information protection is one of the most urgent today. And therefore, it is advisable to start work on the opening of special departments of information security in the leading universities of the country. Also it is necessary to cooperate with industrial enterprises to determine the necessary elective disciplines and to include these elective disciplines in the educational curricula of universities in accordance with the needs of the market.

2 MATERIALS AND RESEARCH METHODS

In the period from January to March of this year, the content of the programs (EP) of the Zhetysu University named after I. Zhansugurov was reviewed with the purpose of evaluating the level of teaching the basics of information security to students.

Also, during this period, a survey was conducted in the form of a questionnaire among students on information security issues. The questionnaire was held among 3-year students of the educational programs 6B06102-"Information Systems", 6B06101-"Informatics" 6B04101-"Economics" and 6B04101-"Accounting and Audit".

The purpose of the survey was to establish the degree of students' knowledge in the field of information security.

The survey was conducted on the following questions:

1. How do you understand information security at the national level?

2. What is information security?

3. What types of information security do you know?

4. Where, in the first place, do you look for and from what sources do you get information?

5. What types of repositories do you use for your information?

6. What information security threats have become relevant over the past year?

7. What methods of protection do you know?

8. Do you use information security methods when you go to social networks?

9. Are you familiar with understanding Phishing?

10. Do you know what to do in case of information leakage?

11. What social networks do you use?

12. How much do you use online banking services?

13. Do you check the information received on the web?

14. Do you know how to protect yourself on social networks?

15. Did you know that it is prohibited by law to post and use information belonging to other people without their consent?

16. Did you know that your personal data can be stolen and used?

3 REASEARCH RESULTS AND THEIR DISCUSSION

The analysis of the University EP showed that information security issues with varying degrees of completeness and detail were reflected in the curricula and training programs for IT specialists, in such educational programs as 6B06102- "Information Systems", 6B06103- "Architecture of Information Systems" and 6B06101- "Informatics". Students, according to the EP, study the following disciplines: "Information security and information protection", Innovative methods of protecting digital information, Digital information security.

When studying these disciplines, laboratory works are carried out with the help of educational and laboratory equipment, such as "Access control systems" and "Cryptographic systems".

In the discipline of "Access control systems" students get acquainted with the programming of contact smart cards and the construction of an access control system (ACS) based on contact smart cards; master the construction of access control systems based on contactless smart cards; acquire skills in setting up equipment for biometric authentication; get acquainted with the basic principles of biometric authentication systems; exploring two-factor authentication using an eToken to log into the Windows operating system; get acquainted with

iButton technology, learn to program the controller; get acquainted with the work of the intercom.

For cryptographic systems, they acquire the skills of using the OpenSSL software product to apply encryption and hashing algorithms, study the DES and RSA algorithms; study the structure of the X.509 certificate and the formats DER, PEM; get the skills of using the GnuPG software product for managing keys and PGP certificates, study the principles of the web of trust, the ISAKMP framework; get the skills of building crypto tunnels in Linux, the appointment of crypto containers; gain the skills to create encrypted file systems in Linux, learn the limitations of encrypted block devices; get the skills to work with the tripwire / aide file integrity control system, with the stunnel utility.

Students of the EP 6V01505- "Informatics", which is part of the EP group - training of teachers of informatics, study the course "Information security in the social environment."

The educational programs of other specialties study the information security issues solely within the ICT course, which significantly limits the consideration of the problem and needs to be adjusted. For such EPs as 6B04101- "Economics", 6B04103- "Accounting and Audit", 6B04105- "Information Resources Management", 6B04201- "Jurisprudence", the computer-related disciplines only partially cover the information security issues and it is done by the following disciplines: "Application of digital technologies in economy and business "," Information law of the Republic of Kazakhstan "[6].

Information security questionnaires among students showed the following results:

To the question "Where, in the first place, do you look for and from what sources do you get information? 92% of respondents replied "on the Internet", 2%, replied "on radio and television" and 6% replied "in an educational institution and in scientific, educational, fiction, technical literature".

To the question "How do you understand information security at the national level?" 56% of the respondents answered "the state of protection of the individual, society and the state from internal and external threats", 28% replied "the level of protection of the individual and society, mainly from internal threats of a generally dangerous nature", 16% replied "prevention of harm inflicted on state structures".

To the question "Do you use information security methods when you go to social networks?" the answers were as follows: yes, I try to use all possible methods of information protection - 45%; yes, I closed access to all my social networks and accounts

for outsiders - 12%; I do not consider it necessary - 25%; I would like to, but do not know how to do it - 18%.
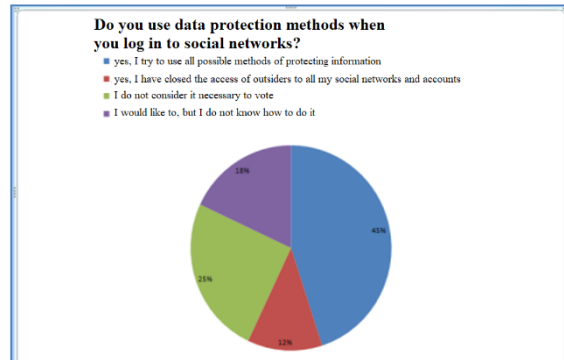

Figure 1: Diagram of the answers to the question Do you use information security methods when you go to social networks?".

To the question "What methods of protection do you know?" the students answered in the following way: the password is set - 42%; restriction of access to this or that information - 23%; user authentication - 17%; personal information on my computer is not well or well protected - 14%; I don't know - 4%.
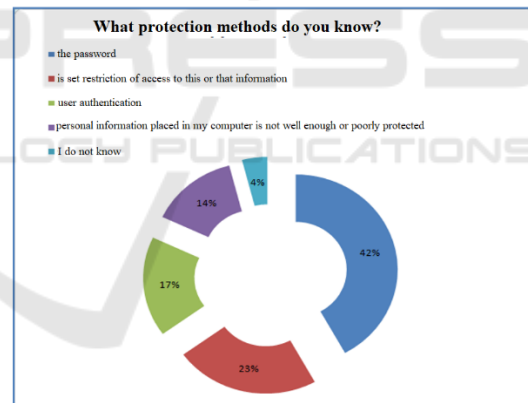

Figure 2: Diagram of the answers to the question "What methods of protection do you know?".

To the question "Do you know how to protect yourself on social networks?" 29% answered that they know well how to protect themselves on social networks; 18% do not know, 24% will turn to a specialist; 18% are sure that if you behave correctly in social networks and do not respond to messages from suspicious people, then there is no need to see a specialist; 7% don't know.

To the question "Do you know what to do in case of information leakage?" the respondents' answers were as follows: did not think about it - 26%; don't know -22%; I will seek help from a specialist -22%;

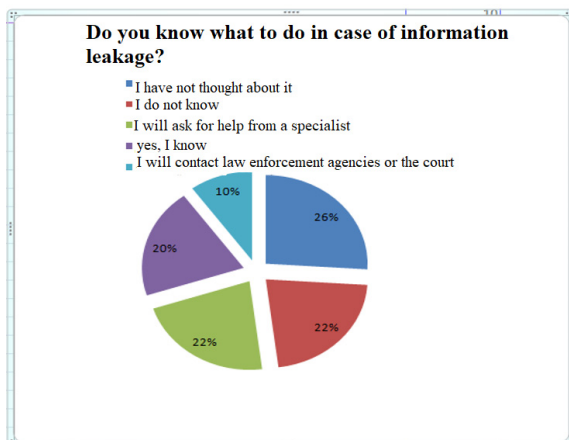yes, I know - 20%; I will go to law enforcement agencies or the court -10%.

Figure 3: Diagram of the answers to the question "Do you know what to do in case of information leakage?".

To the question "What threats to information security have become relevant over the past year?" 19% of students believe that this is the activity of hackers, 20% - negligence of system administrators. specialists, 11% - non-professionalism of employees of the service / information security bodies, 32% - Internet fraud, 18% - computer viruses.

The analysis of the survey showed that the students of the educational programs "Information Systems" and "Informatics" are better prepared in the field of information security and information protection.

The importance of the problem of information security increases with the growth in the scale of using modern information and communication technologies, which are the technological basis of globalization processes in all spheres of life of modern society. Today information and communication technologies are an important component of our lives, and, therefore, each individual in his professional activity should have the knowledge of information security.

Therefore, the introduction of training in the basics of information security is necessary in all educational programs, especially for students in the field of economics. It is especially important nowadays when we witness the rapid development of electronic payment systems. It leads to a bigger percentage of economic activity being carried out in an electronic environment which is associated with increased level of information risks.

The system of teaching the basics of information security should be characterized by complexity, continuity, and adaptability. The content of training

in the basics of information security and information protection can be built on the basis of a system analysis of the main objects of the subject area of future professional activity. The result of such an analysis should be the identification of the basic objects of study, their interrelationships, methods and technology for their study.

4 CONCLUSIONS

The tasks of increasing literacy in the use of information and communication technologies (ICT), the use of standard methods of protecting information when working on a personal computer, in local and global networks, remain relevant. Therefore, training in the field of information security and information protection needs significant improvement and development at subsequent stages of education.

For EP that train specialists whose professional activities are related to ICT, it is necessary to include the discipline "Fundamentals of Information Security" in the structure of the studied courses (university component or component of choice), the main goal of which is to increase the effectiveness of training specialists in ensuring information security when using ICT in the field of professional activity. Along with the traditionally considered aspects of information security and information protection, it should reflect the methodological, cultural, legal, organizational and managerial aspects of information security.

REFERENCES

Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V "On Informatization" (with amendments and additions as of 01/02/2021)

Melnikov, V.P., Kleimenov,, S.A. and Petrakov A.M. (2012). *Information security and information protection:* Textbook for students. higher. study. Institutions, 6th ed. sr. - M .: Academy, 336 p.

Polyakov, V.P. (2006). On the training system for the basics of information security. Finance: theory and practice, (3): 125-136.

Kaie Maennel, Sten Mäses, Stefan Sütterlin, Margus Ernits, Olaf Maennel, Using Technical Cybersecurity Exercises in University Admissions and Skill Evaluation. *IFAC-PapersOnLine,* 52(19): 169-174.

Steven Furnell, 14 October 2020. The cybersecurity workforce and skills, *Computers & Security*, 100: 102080.

https://lenta.inform.kz/kz/kakie-specialisty-mogut-vsegda-nayti- rabotu_a3146725

Mari Karjalainen, Mikko Siponen and Suprateek Sarker (2020). Toward a stage theory of the development of employees' information security behavior, *Computers & Security*, 93, 101782.

Seitkulov E.N. (2016). *Information Security of the Republic of Kazakhstan: State and Prospects*.

Ge Xiao-yan, Yuan Yu-qing and Lu Li-lei, (2011). An Information Security Maturity Evaluation Mode, *Procedia Engineering*, 24, pages 335-339.