Formation of Competencies in the Information Security and Information Protection Field within the Framework of the Federal Project "Human Resources for the Digital Economy"

Elena V. Chernova[1][a] and Andrei S. Dokolin[2][b]
[1]*Power Engineering and Automated Systems Institute, NMSTU, 38 Lenin avenue, Magnitogorsk, Russia*
[2]*Municipal educational institution "Secondary school № 28", 141/4 Karl Marx Avenue, Magnitogorsk, Russia*

Keywords: Information Security, Information Protection, Education, Professional Training.

Abstract: The problem of preparing the user to understand the information security essence, as well as the basic competencies formation for the protection of personal and professional information, was particularly acute during the 2020 pandemic, in the context of the transfer of all activities to a remote format. The paper presents the content of the professional development program "Information Protection", developed within the framework of the federal project "Personnel for the digital economy" for students who have higher education within the existing qualifications and don't have specialized education in the field of information security and information protection. The descriptors of the formed competencies with their characteristics are described. The educational and thematic plan of the course is given. The topics studied, the goals of practical classes and tasks are revealed, and the specifics of the tasks offered to the students are described.

1 INTRODUCTION

The federal project "Personnel for the digital economy" of the national program "Digital economy of Russia 2024" is designed to assist citizens in mastering the key competencies of the digital economy, ensuring mass digital literacy and education personalization (Human resources for the digital economy, 2021). The national program covers a number of main areas: human resources for the digital economy; information infrastructure; information security; digital technologies; artificial Intelligence; regulatory regulation; public administration; digital region; industry areas.

Today, the society has a great need for highly qualified personnel capable of ensuring information security and information protection in professional and personal life. The objectives of the "Information security" direction are to achieve the following indicators in 2024: "50% of citizens who have increased their literacy in the information security field, media consumption and the use of Internet services" and "97% population who have used information security tools out of the total population who have used the Internet in the last 12 months». According to an analytical report from Positive Technologies for the third quarter of 2020, the share of attacks using social engineering methods, as well as malicious software, remains the highest, relative to other methods of obtaining unauthorized access to protected information (Figure 1) (Current cyber threats: III quarter of 2020, 2020). At the same time, it should be noted that most often attackers use "template" attack schemes and raising awareness of company's employees and individuals can already provide a sufficient level of protection against leaks and loss of information generated by these ways.

[a] https://orcid.org/0000-0001-6664-7614
[b] https://orcid.org/0000-0002-5838-4567

Chernova, E. and Dokolin, A.
Formation of Competencies in the Information Security and Information Protection Field within the Framework of the Federal Project "Human Resources for the Digital Economy".
DOI: 10.5220/0010617500003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 61-67
ISBN: 978-989-758-531-9; ISSN: 2184-9862

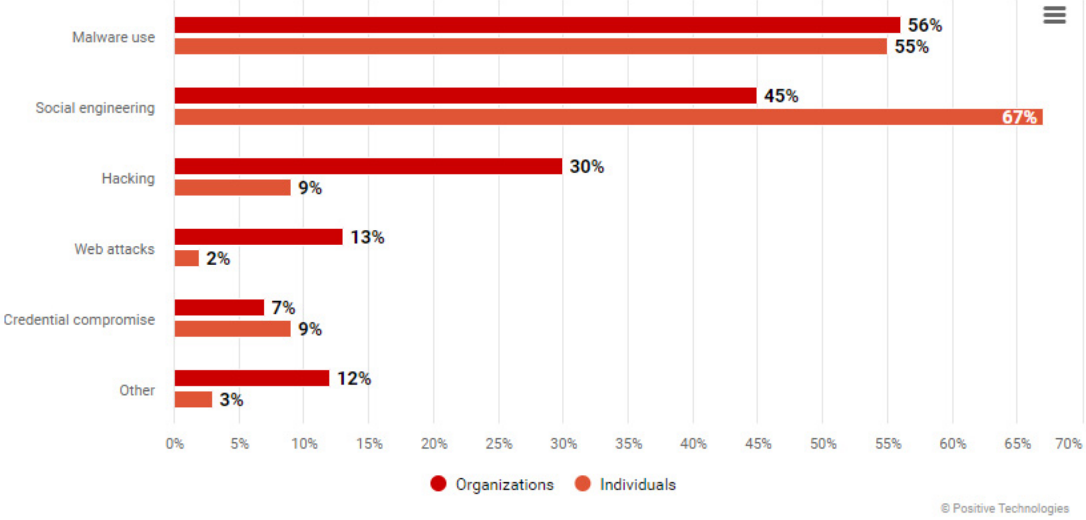

Figure 1. Share of attacks using social engineering methods, Q3 2020.

At the same time, it should be remembered that the information protection process is a complex and specific system and it is necessary to train a non-core employee in the basics of data protection, taking into account the most common vulnerabilities and threats to personnel. As the specialists of Positive Technologies note: "that any company can be hacked in one way or another during an attack, and the task of information security is to prevent the attacker from causing any significant damage" (Cybersecurity 2020-2021, 2021). At the same time, it is obvious that "the personnel involved in information relations, and all employees of the organization are such in one way or another, is a potential violator of information security – intentionally or not" (Zakharov, 2019). At the same time, "by improving the personnel skills in the field of information security, the company can significantly reduce the risk of information security violations. It is not for nothing that personnel training is one of the main requirements of the international information security management standard ISO/IEC 27001:2005" (Zakharov, 2020) One of the current problems is the openness of user data in social networks: "more and more users who sit on social networks want to expose their lives, while publishing a lot of information about themselves and their professional activities, and sometimes going beyond the boundaries of normality" (Chernova, 2020).

The need to raise the level of the user and the specifics of teaching adults the information security basics has been repeatedly discussed by both specialists in the information security field and teachers of higher education. At the same time, it's noted that there is a need "to produce not just a specialist, but one who is ready to engage in the use of new technologies within the framework of his profession, to be adapted to the changing conditions of the working environment, as well as capable of decision-making and consulting activities and implementation of the concept “lifelong learning” assumes consideration of continuing professional education as a multilevel system in which all knowledge, skills and competences are results of training and taxonomic by nature" (Chusovitina, 2016). However, "today, there are a number of problems in the education system that cannot be ignored when building an educational trajectory: a decrease in the number of applicants, the growth and variability of employers' requirements for the content of future employees training, changes in the labor market» (Chernova, 2013). "At the same time, it should be remembered that the information protection process is a complex and specific system, and it is necessary to train a non-core employee in the basics of data protection, taking into account the most common vulnerabilities and threats to personnel" (Chernova, 2020).

2 COURSE "INFORMATION SECURITY"

We have developed a training program for the digital economy "Information security", while the program is aimed at the average user who doesn't have specialized knowledge in the information security and information protection field.

As a basis for developing the course, we analyzed modern professional standards in the information protection field and selected professional standard No. 843 "Specialist in information protection in Automated systems" (Order of the Ministry of labor and social protection of the Russian Federation No. 522n of 15.09.2016) as the main one. Based on the work activities described in this standard, we have analyzed and identified the basic knowledge and skills necessary for an ordinary user to maintain the required level of information security in their workplace according to their professional qualifications.

To study under the program, the student must:

- know the subject area; basic principles of working with information, the basics of information search, basic regulations of the Russian Federation;
- be able to: install and study the required software, perform information search;
- master the skills of confident work on the computer.

The purpose of the program is to improve the professional level of students in the information security field within the existing qualifications.

During the training, the students learned not only the basics of ensuring the information protection, but also performed practical work to consolidate their knowledge. Practical tasks cover diverse areas of activity, which will allow students to apply the acquired knowledge and skills in everyday life after completing the course. At the same time, the information submission level is focused on a non-specialist in applied computer science, the level of a confident PC user is sufficient to complete tasks and then use the proposed methods.

The educational-thematic plan of the advanced training program is designed for 72 hours and includes a curriculum and a training (working) program of advanced training.

A competencies passport has been developed, which includes the modern realities of the ensuring information protection and information security process.

Competence name: administration of information security systems of automated systems.

Specifying the competence type: professional.

Competence definition, content and main essential characteristics: competence refers to the ability to ensure the protection of information in an automated system, taking into account the requirements set.

The listener must:

To know:

- software and hardware mean of information protection of automated systems;
- basic measures to protect information in automated systems.

Be able to:

- install and configure software tools to meet the requirements for ensuring information security;
- use cryptographic methods and information security tools in automated systems;
- analyze events related to information security in automated systems.

Possess:

skills of using software tools to solve the tasks set for information protection.

Descriptor of knowledge, skills and abilities by level.

Initial level (The competence is not sufficiently developed. Partially demonstrates the skills that are part of the competence. Tries, strives to show the necessary skills, understands their need, but doesn't always succeed).

Knows: the basics of computer literacy.

Able to: install and configure software according to the specified parameters.

Possesses: the skills of confident PC use to solve tasks.

Basic level (Confidently possesses the skills, is able to show the appropriate skills in situations with elements of uncertainty, complexity).

Knows: about the problems of ensuring the protection of information.

Able to: apply software tools to ensure the protection of information to solve the tasks (destruction, concealment of information, etc.).

Possesses: the skill of selecting ready-made solutions for the required information security situation.

Advanced level (Possesses complex skills, is able to actively influence what is happening, show appropriate skills in situations of increased complexity).

Knows: software and hardware information security tools.

Able to: formulate requirements for ensuring the protection of information: set goals and objectives.

Possesses: the ability to work with programs and algorithms for cryptographic information protection.

Professional level (Possesses complex skills, creates new solutions to complex problems with many interacting factors, offers new ideas and processes, is able to actively influence what is happening, show appropriate skills in situations of increased complexity).

Knows: methods and means of information protection.

Able to: select, install, configure and apply special software tools to ensure the information protection for solving tasks (destruction, concealment of information, etc.).

Possesses: the ability to formulate requirements for ensuring the information protection and determine the ways to achieve them: set goals, objectives, select methods and means of protecting information in the problem area.

Competence name: ensuring the information security systems operability in the event of emergency situations.

Specifying the competence type: professional.

Competence definition, content and main essential characteristics: competence refers to the ability to restore automated systems after software failures and breakdowns.

The listener must:

To know:

- organizational measures to protect information.

Be able to:

- classify and evaluate information security threats;
- apply software tools to ensure data security.

Possess:

- skills of using software tools for recovery after information processing systems failure.

Descriptor of knowledge, skills and abilities by level.

Initial level (The competence is not sufficiently developed. Partially demonstrates the skills that are part of the competence. Tries, strives to show the necessary skills, understands their need, but doesn't always succeed).

Knows: the main threats to information security and ways to prevent them.

Able to: determine the requirements for the organization of the protecting documented information process.

Possesses: an understanding of the unauthorized access to data carriers' methods.

Basic level (Confidently possesses the skills, is able to show the appropriate skills in situations with elements of uncertainty, complexity).

Knows: the main threats to information security and the intruder model.

Able to: create a strong and resistant to hacking password.

Possesses: an idea of how to protect information from status violations.

Advanced level (Possesses complex skills, is able to actively influence what is happening, show appropriate skills in situations of increased complexity).

Knows: advanced software for storing information required status.

Able to: select, configure, and use advanced software to store information required status.

Possesses: the ability to use specialized software for data recovery.

Professional level (Possesses complex skills, creates new solutions to complex problems with many interacting factors, offers new ideas and processes, is able to actively influence what is happening, show appropriate skills in situations of increased complexity).

Knows: various resources to check the protection level of the information availability and confidentiality status.

Able to: select, configure and use specialized software for data recovery.

Possesses: the ability to select resources to solve the tasks set for the recovery of automated systems after a failure or to prevent a failure.

3 THEMATIC PLANNING OF THE "INFORMATION SECURITY" COURSE

The course uses the theoretical aspects presented in the textbook by Chernova E.V. "Information security of the person" (Chernova, 2020). According to the competency passport, the following thematic planning was proposed:

Theme 1. The essence and concept of information security (10 hours)

Basic concepts. The value of information security for information relations subjects. The concept and essence of information security. Objectives and conceptual foundations of information security. Criteria, conditions and principles for classifying information as protected. Carriers of protected information.

Practical work. Reliability and accuracy of information. Services for determining the reliability of a resource on the Internet.

The goal is to learn how to apply existing methods of analyzing information for its reliability and accuracity.

Task 1. Find the resources of the Federal state agency, Regional state agency, a news resource - to substantiate their reliability and accuracity using the proposed verification services.

Task 2. Threats to the availability, integrity and confidentiality of personal information.

Task 3. Letters of happiness, mobile applications, manipulation of user actions, fake news.

Note: for the work, obviously reliable resources were selected to demonstrate to students what a trusted resource should look like. For the rest of the tasks, special cases were developed that demonstrate the current problems of ICT (Information and Communication Technologies) users.

Theme 2. Threats to information security (10 hours)

Threats to information security and information protection. Destabilizing effect on the protected information. Classification of information security threats types by various criteria. Unauthorized access to information.

Practical work. Definition of threats and the intruder model of the domain. Assessment of security risks. Develop recommendations for risk reduction.

The goal is to analyze the subject area in terms of identifying threats in this area and developing recommendations for their prevention.

Task. Analyze the presented subject area, identify threats, develop a model of the intruder, and assess the risks of a security breach according to the specified parameters.

Note: students were offered both standard subject areas (library, publishing agency, etc.) and unusual, fantasy areas (for example, a real estate agency on Mars, the Marvel Corporation, the Ministry of Magic, and others). This approach has shown that the rules and norms of information security and information protection are applicable to any subject area.

Theme 3. Administrative level of information security (10 hours)

Security policy. Security program. Risk assessment and basic level of protection.

Practical work. Protection of information from unauthorized access.

The goal is to develop basic knowledge, skills and abilities in the field of personal information protection on a personal computer and the resources used.

Task 1. Learn the configuration of your computer using the program.

Task 2. Use the suggested program to check which programs on your PC are not licensed.

Task 3. Study the Wi-Fi network available to you with the help of the proposed programs. What vulnerabilities were discovered?

Task 4. The program network security monitor and firewall to monitor your network.

Task 5. Online password generation services and password generation programs. Browser Features.

Task 6. Online password verification services for resistance to hacking.

Task 7. Online and offline password managers. Storing passwords in the browser.

Task 8. Mass mailing of emails with the hiding of the address book and a personal appeal to the addressee.

Note: for work, students were offered free software, characterized by information security specialists as reliable. Also, the work offers resources that reflect the current state of the problem of information security and created by leading security practitioners.

Theme 4. Software tools for information protection (18 hours)

Protection of software from unauthorized access. A brief overview of the existing means of protecting information from unauthorized access on the market. The task of protecting against unauthorized interference and authentication hardware. Deleting information with the specified requirements.

Practical work. Protection against unauthorized access to information.

The goal is to study the possibilities of controlling and preventing unauthorized access to information using various methods.

Task 1. Creating and working with token baits.

Task 2. Ways to close access to a folder in Windows.

Task 3. Vulnerability analysis of Internet logins.

Task 4. Protection of information in documents: password, prohibition of changes, templates.

Task 5. Data recovery using software.

Task 6. Permanent deletion of information, low-level formatting.

Note: for work, students were offered free software, characterized by information security specialists as reliable. Methods and recommendations from leading information security practitioners were also used. The methods and tasks under consideration range from easy ones, performed by the basic tools of the operating system, to advanced ones, using specialized software and / or program code.

Theme 5. Cryptographic methods of information security (10 hours)

Cryptography methods. Means of cryptographic information protection. Cryptographic transformations. Encryption and decryption of information. Digital signature. Steganography.

Practical work. Cryptographic information protection.

The goal is to study the methods of cryptographic information protection used to solve various problems of the professional field.

Task 1. Study of various encryption methods: replacement method, Cardano method, permutation method.

Task 2. Creating hash functions.

Task 3. Steganography: hiding data in graphics and music files. QR codes.

Examples of control tasks and cases

How can you build a comfortable and secure work at the workstation: protection against unauthorized access with a computer left unattended?

Ensuring the safety of information in application packages (for example, MS Office) in the event of a failure.

Protection against unauthorized access to files stored on the hard disk when: differentiating access between different users; the inability to differentiate access between different users.

The user constantly uses media from various places, while: the user's computer is not connected to the Internet; the user's computer is connected to the Internet.

Using three different methods of hiding information, encrypt the message "Information is the queen of the world".

The flash drive is infected with malware that leaves only shortcuts to folders available. After the antivirus program was running, the shortcuts were removed. Describe the recovery procedure in any way.

You mistakenly deleted the files you needed, and the trash was also emptied. How can you restore files? Describe the recovery procedure in any way.

Describe the low-level formatting procedure. What is it for?

Describe the different ways to delete a file from your computer, without using specialized software, what is the special feature of each?

Describe the mechanism for deleting a file from the computer at the machine level.

Describe the steganographic methods of hiding information in a computer image: exif, geo-tag, archive, watermarks.

Learning tasks (cases), other practice-oriented forms of assignments

It is known that the manager of the company Alina has a personal email account, and that she uses social networks (Vkontakte, Odnoklassniki, Facebook, etc.). At the same time, she closes the browser without pressing the "exit" button, uses Internet Explorer, has 1-2 simple passwords for all resources, goes online mainly from the workplace sometimes from home, all social networks are linked to one email box.

Identify risks related to information security aspects: integrity, availability and confidentiality.

Formulate recommendations for Alina on protection against information security threats.

Ekaterina received an email with the following message: "Hello, Vladimir! You have made a request to restore the data of the electronic wallet "WebMoneySet". Your username: vladimir1986. Your password:236834vm. To manage your account, install the plugin for making money transactions in the attachment". The *exe file is attached to the email.

What actions should Catherine take in this situation?

Is there any method(s) of psychological influence used in this situation? If so, which one? Explain your point of view.

George has more than three years of experience in the IT industry, he is now looking for a job and has posted his resume on several Internet services. After some time, he was contacted by A.A. Svetlov, who introduced himself as an HR manager of "Infosoft". To decide whether to invite George for an interview or not, the employer wants to test his skills with mobile programs. A.A. Svetlov offers to download a special program from the link and demonstrate your skills. George downloads the application, performs the task of the employer, but he is not invited to the interview. After some time, it turns out that the malware allowed the attackers to take possession of George's funds from an account linked to a mobile bank.

1. What errors can be identified in the information behavior of George?
2. How to act in this situation?
3. How to avoid similar situations later?

4 COURSE COMPLETION RESULTS

In the process of the course students were asked to study the specialized software tools and resources to simplify the procedures for protecting private information from unauthorized access, loss and leakage. The listeners got acquainted with the resources for checking personal data-leaks of passwords, logins. We mastered the resources and programs for creating strong passwords and storing them. We studied the features of deleting information using standard OS tools and special programs, and the key characteristics of these procedures.

The course developed by us received the qualification of a level 3 course at the 20.35 University: "the third level is the ability to perform effective and productive activities within this field" (Zakharov, 2019). In the first stream, 11 people were trained in the course, all received certificates of advanced training. It should be noted that not all students were specialists in the field of ICT, however, in general, reviews of the course indicated that the tasks were written competently and interesting for people of different levels of involvement in the information security field.

5 CONCLUSIONS

Modern methods of processing, transmitting and storing information have contributed to the emergence of threats associated with the possibility of loss, distortion and disclosure of data addressed to or belonging to end users. Therefore, it is necessary to teach the average user the basics of ensuring the information protection in their personal life and professional activities, thereby reducing the level of their involvement in the information security violations processes.

REFERENCES

Chernova, E.V. (2013). *The experience of academic partnership between the university and software manufacturers in the field of information security as a tool for improving the students competitiveness.* Fundamental study, 111-115.

Chernova, E.V. (2020). I*nformation security of a person.* Moscow: Urait publishing house.

Chernova, E.V. (2020). Threats to information security when employees work in social networks. *Modern management model: problems and prospects: materials of the All-Russian (national) scientific and practical conference*, pages 43-48. Magnitogorsk: Nosov Magnitogorsk State Technical University publishing house.

Chusovitina, G.N. (2016). Elaboration of a frame model for intensification and managing requirements to learning outcomes in regional systems of continuing professional education. International Review of Management and Marketing, 190-197.

Current cyber threats: III quarter of 2020. (2020, November 16). Retrieved from Positive Technologies: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/

Cybersecurity 2020-2021. (2021, January 28). Retrieved from Positive Technologies: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021/

Human resources for the digital economy. (2021, February 2). Retrieved from Ministry of digital development, communications and mass media of the Russian Federation. https://digital.gov.ru/ru/activity/directions/866/

Polushkin D.P. (2017). *The motivation of high school teachers in the formation of their own competencies in the field of information security*. Security & Future, 21-22.

Zakharov, S.Yu. (2019). The role of personnel in maintaining the information security of the organization. *Information technologies in science, management, social sphere and medicine: collection of scientific papers of the VI international conference*, pages 557-560. Tomsk: Tomsk polytechnic university publishing house.

Zakharov, S.Yu. (2020). Information security training system for personnel to improve the competitiveness of the organization. *Modern management model: problems and prospects: materials of the All-Russian (national) scientific and practical conference*, pages 43-48. Magnitogorsk: Nosov Magnitogorsk State Technical University publishing house.