Building Competencies in the Information Security Field for Future Bachelors of Applied Computer Science

Elena V. Chernova[a], Irina V. Gavrilova[b] and Marina V. Romanova[c]
Power Engineering and Automated System Institute, Nosov Magnitogorsk State Technical University, Lenin Avenue, Magnitogorsk, Russia

Keywords: Bachelor's Training, Information Security, Applied Computer Science, Competence-Based Approach.

Abstract: The article is devoted to solving the problem of developing a competencies model in the information security field for bachelors in the Applied computer science direction. The development of information technologies and the Russian higher professional education system leads to a consistent transformation of the idea of the competencies necessary for a bachelor of applied computer science in the field of information security. Taking this into account, as well as studying the experience of training future bachelors in other Russian universities, a competency model was developed, which formed the basis for the formation of the Information Security discipline content. The article presents the descriptors of the formed competencies. The authors believe that bachelors of applied computer science should be able to use the basics of legal knowledge, regulatory documents, international and domestic standards in the information security field, design and build secure information systems (IS), and estimate the costs of ensuring information security at different stages of the IS life cycle. Special attention is paid to the teaching methodology, the main elements of which are problem-based learning, as well as the methodology of "thick and thin questions".

1 INTRODUCTION

In recent years, the active development of information technologies has made a large number of changes in all areas of social life. Digitalization and the transfer of many processes to online has raised the issue of building the competence of future specialists of any profession in the information security field more acutely. This idea has been confirmed at the state level and is reflected in the Information Security Doctrine of the Russian Federation, which emphasizes the increasing role of the information sphere, which is a set of information, information infrastructure, entities that collect, form, distribute and use information, as well as the system of regulating the public relations that arise in this process (Gorbunov, 2012). The importance of the problem of training future specialists to ensure information security was raised in the works of teachers related to the disciplines of information security and information protection (Chusavitina et al., 2018; Chernova et al., 2017; Chernova, 2019; Gorbunov, 2012).

In our work, we will consider the building competencies in the information security field for future specialists of "Applied computer science".

The direction of training "Applied computer science" appeared in 2000, when the state educational standard of higher professional education (SES HPE) was approved in the specialty 351400 "Applied computer science (by field)". In this standard, mandatory disciplines and their summary were fixed, while "Information security" was assigned to the special disciplines block. Already in this standard, the following thematic blocks were traced:

1) standards in the field of information security and information protection (IS&IP);

2) information security threats and their classification;

3) ensuring IS&IP at the state, administrative and information technology levels.

[a] https://orcid.org/0000-0001-6664-7614
[b] https://orcid.org/0000-0002-4283-5810
[c] https://orcid.org/0000-0003-0229-4463

Chernova, E., Gavrilova, I. and Romanova, M.
Building Competencies in the Information Security Field for Future Bachelors of Applied Computer Science.
DOI: 10.5220/0010617700003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 74-80
ISBN: 978-989-758-531-9; ISSN: 2184-9862

The process of increasing information resources, processing big data, and accelerating innovative and technological changes has brought the Russian economy and the Russian market into constant motion. Any company under the external and internal macro- and microparameters influence must constantly change the strategies, organizational structures and management apparatus of enterprises in order to keep up with the trend. New trends have affected the requirements for personnel and their training. "Personnel is an important factor for ensuring the stability of the company's work, as well as the importance of hiring qualified personnel who have competencies not only in their professional field, but also in important areas for the information society – information culture and information security skills" (Zakharov, 2019). «Safety of functioning of any business depends on the level of understanding by management of the importance of implementation of activities in the company of it solutions related to information protection and information security.» (Chernova, Gavrilova, Romanova and Dokolin, 2017).

2 THE METHODOLOGICAL RESEARCH APPARATUS

The purpose of our work is to develop a competency model in the information security field for bachelors of Applied computer science. To achieve this goal, we primarily relied on a competence-based approach.

Despite the fact that this approach has been studied and used in scientific research and practice since the early 2000s, the definition of the basic concepts of this approach is used ambiguously. Thus, the concepts of "competence" are considered by scientists both as the person's ability (A.M. Choshanov, 1996), and as his experience (N. Chomsky, 1972), and as a set of factors that combine in a person (Khutorsky and Elkonin, 2003). If we consider the definitions that scientists have given to the concept of "competency " and compare them with the definitions of "competence", we can see that the former more often describes behavioral aspects, while the latter describes functional and qualitative characteristics of the individual (Troyanskaya, 2016). As the study of a new approach to education in Russia, its application began in the educational standards (FSES).

On February 5, 2010, the federal state educational standard of higher professional education (FSES HPE) was registered in the training field 230700 Applied computer science (qualification (degree) "bachelor"), which did not contain requirements for the training content in the discipline "information security", but described the general cultural competency GCC-13: "able to understand the essence and significance of information in the modern information society development, to be aware of the dangers and threats that arise in this process, to comply with the basic requirements of information security, including the protection of state secrets" (11) - in fact, the same training result was described as in the previous standard.

In 2015, the federal state educational standard of higher professional education (FSES HPE) was adopted in the training field 09.03.03 Applied computer science (13), in which the competencies were revised, while information security is mentioned only in one, professional competency: to have the ability to take part in the organization of IT infrastructure and information security management (PC-18). The level of training in information security should be sufficient so that the graduate can take part in its management throughout the organization, i.e. simple knowledge of terminology is not enough.

In 2017, the federal state educational standard of higher education – bachelor's degree in the training field 09.03.03 Applied computer science (FSES HPE 3++) was adopted, in which "GPC3" is mentioned among the general professional competencies - is able to solve standard tasks of professional activity on the basis of information and bibliographic culture with the ICT use and taking into account the basic information security requirements" (15), while professional competencies are recommended to be linked to the professional standards "Programmer", "Information Systems Specialist", "Project Manager in the information technology field", "Head of Software Development", and "System Analyst". Despite the fact that knowledge of the organization information security basics is considered mandatory only in one of the listed standards, namely in the standard "Information systems specialist", the bachelor of Applied computer science should be prepared for this professional activity, and, therefore, the discipline "Information security" should be provided for by the plan for their preparation.

Based on the above, we believe that competence in the information security field is an integrative professional and personal characteristic of an IT specialist, including a stable motivation and interest in self-development in the information security field, knowledge of the information security theoretical foundations, as well as skills, abilities and experience in successfully protecting professionally significant

information and countering threats to information security in professional activities. This concept includes a set of competencies that need to be identified, structured and justified.

The Federal educational and methodological association in the system of higher education in the specialties and directions enlarged group (EGSD) "Computer science and computer engineering" recommends the following mandatory topics within the discipline "Information security»:

- information security in the Russian national security system;
- information war, methods and means of its conduct;
- criteria for the computer systems security;
- protection of information processed in information systems;
- protection of automated systems (AS) and computer equipment (CE) from external electromagnetic influence.

A comparative analysis with the thematic blocks of the earliest FSES HPE shows that they practically don't differ from its recommendations.

All of the above allows us to talk about the need to develop a model of a tabular form that reflects the complex of competencies necessary for a modern specialist in the information security field, which must be built by bachelors in the Applied computer science field. To solve this problem, scientists use two approaches: the classical approach and the methodology for developing the FSES.

The classical approach to competencies was presented in their works by Spencer and Spencer, who, as a methodology, cited a reference book describing 21 competencies. These competencies mainly relate to the section "Self-concepts". In addition, the authors provided evaluation scales and indicative characteristics of competencies (Troyanskaya, 2016).

Methodology for the FSES development, where the formulation of a competency model is carried out by an expert method. This process consists in compiling a list of job functions, knowledge, skills and qualifications. To work on this list, organizations employees are involved, whose experience can be collected and processed in a questionnaire or interview format. In the future, this list is used to compile a professional standard and is being finalized by a group of experts.

In the study, we used the second approach, isolating from those proposed by the FSES scientists those competencies that reflect the necessary descriptors of the competencies we are considering.

3 RESULTS

Federal State Educational Standards of the 3rd and 4th generations have already been formulated in terms of competencies and give their types - general cultural, professional, professional by type of activity and training. Currently, the scientific and pedagogical literature distinguishes the following key competencies that every person undergoing training should have (Troyanskaya, 2016):

- the ability to independent cognitive activity;
- the ability to independently solve problems in the field of social, labor, social and household activities;
- communication skills;
- the ability to project activities;
- the ability to create a safe and healthy environment;
- the ability to navigate in the surrounding world and create an environment for spiritual development.

We have identified the following competencies to form a set of competencies in the information security field:

- the ability to use the basics of legal knowledge in various fields of activity;
- the ability to use regulatory documents, international and domestic standards in the information systems and technologies field;
- the ability to solve standard tasks of professional activity on the information and bibliographic culture basis with the use of information and communication technologies and taking into account the basic information security requirements.

According to the website "Postupi.Online" (14) in the Russian Federation, training in the "Applied computer science" field is carried out by 179 higher educational institutions. The analysis of the "Information security" working programs of these universities showed that each of them has its own idea of this course content, but all of them in the "To know" section adhere to the lines presented in the first FSES HPE, while often don't coincide in the description of the "Be able" and "Possess" sections. Based on the above, a generalized representation of the competencies formed as a result of studying the discipline "Information security", in our opinion, should look like this.

"To know" section:

- on the legislative, administrative, organizational, software and technical levels of information security;

- basic laws and regulations in the information security and information protection field, measures of the administrative and organizational level of information security;
- basic principles for the development of information security formal models;
- discretionary, mandated, and role-based security policy models;
- the main methods of ensuring the confidentiality and integrity of information; information security services of the software and technical level;
- discretionary, mandated, and role-based security policy models;
- basic information security tools;
- principles, methods and means of solving standard problems, taking into account the basic requirements of information security;
- types and sources of threats to information security when solving standard tasks of professional activity.

"Be able" section:

- choose the right legislative, administrative, organizational, and software-technical measures to ensure information security;
- apply laws and regulations, measures of the administrative and organizational level of information security to organize an integrated information protection system;
- identify current security threats sources when solving standard professional activity tasks
- use information security services of the software and technical level for the design, development and operation of information systems;
- formulate the relevant requirements for information security systems;
- analyze types of attacks and threats to information security.

"Possess" section:

- the ability to search for the necessary information in laws and regulations for the implementation of information security measures;
- developing documentation methods of the administrative and organizational level of information security for the organization of a comprehensive information security system;
- skills in the implementation and operation of information security services at the software and technical level, including skills in solving problems of identification and authentication of the computer system user, as well as typical tasks of ensuring the computer information confidentiality;
- basic skills in building and managing information security systems;
- the skills of choosing and applying measures of the information security legislative level in solving professional activity standard tasks.

Taking into account the identified and described generalized descriptors, a model of the complex of formed competencies in the information security field was constructed as part of the study of the discipline "Information security" for future bachelors of Applied computer science (Table 1).

Table 1: Model of the complex of formed competencies in the information security field.

Structural element of competency	Planned study outcomes
GCC-4 – the ability to use the basics of legal knowledge in various fields of activity	
To know	the main regulatory legal documents in the information security field.
Be able	apply the requirements of regulatory legal documents to solve the educational tasks of the discipline.
Possess	skills of working with normative legal acts, the practice of their interpretation and application on the legal foundations of information security, which are important for the professional training of specialists in the field of information systems and information technologies.
GPC-1 - the ability to use regulatory documents, international and domestic standards in the field of information systems and technologies	
To know	basic regulatory documents, international and domestic standards in the field of information security;
Be able	recognize and discuss international and domestic standards in the information security field.
Possess	skills of working with regulatory documents, international and domestic standards in the information security field, which are important for the professional training of specialists in applied computer science;
GPC-4 – the ability to solve standard tasks of professional activity based on information and bibliographic culture using information and communication technologies and taking into account the basic requirements of information security	
To know	requirements for the protection of certain types of information, ways to protect information in automated data processing systems, global and local networks;

Structural element of competency	Planned study outcomes
Be able	select and use methods and means of information protection
Possess	skills in the use of administrative and procedural levels of information protection;
PC-21 – the ability to assess economic costs and risks when creating information systems	
To know	methods for assessing the economic costs of providing information security at various stages of the information system life cycle;
Be able	evaluate the economic costs of ensuring information security;
Possess	the methodology for estimating the total cost of ownership for the information security subsystem;
APC-2 – ability to participate in project management, IT-infrastructure organization and information security management	
To know	classes of the procedural level measures of ensuring information security (personnel management; physical protection; maintenance of operability; response to security violations; planning of recovery operations);
Be able	determine requirements and measures in the information security field by types of information system support;
Possess	administrative, procedural, and software-technical measures to ensure information security at various stages of the information system life cycle;

The process of building competencies in the information security field for bachelors in the "Applied computer science" direction is complex and multifaceted. As an example, let's consider it based on the APC-2 (the ability to take part in project management, organization of IT-infrastructure and information security management) in the process of studying the discipline "Information security". To achieve the planned results, we used various innovative forms and methods, which are presented in Table 2 in accordance with the stages of this process and the tasks to be solved at each stage.

Table 2: Building competence (APC-2) in the course of studying the discipline "Information security".

Stages of competency formation	The problem solved in the process of mastering the discipline	Forms, nature of educational and educational-professional assignments, type, volume and forms of control
Diagnostic	Find out the level of formation to determine the requirements and measures in the information security field by types of information systems support, the level of educational motivation, motivation for the profession, personal characteristics of educational activities	Incoming control: preparation of material on the technology "Thin and thick question" on the topic "Legislative and regulatory framework for information security"
Motivational-value	Formation and development of competency in the information security field	Laboratory workshop Participation in the educational and research project "Classification of threats in the subject area"
Theoretical	Formation of the competency content – APC-2	Preparation of a message, presentation, selection of video materials (optional) "Information security policy", " Modern malware for PCs and mobile devices» Participation in the educational and research project "Classification of threats in the subject area"
Practical	Formation and development of skills and practical actions – APC-2	Laboratory workshop Participation in the educational and research project "Classification of threats in the subject area"
Control and analytical	Verification, analysis, assessment, correction of the formation of APC-2	Laboratory workshop Participation in the educational and research project "Classification of threats in the subject area"

During the seminars, the methodology of "Thin and thick questions" was used. The use of "thin" and "thick" questions has three goals: ability to consistently move from information to reasoned disclosure of the topic. Strengthen the skill of formulating questions. Teach a culture of discussion, respect for other people's opinions. The formed ability to correctly ask questions and answer them develops the intellect of the student, helps further self-education. Learn to argue, defend your position reasonably. The text, considered from the point of view of "thin and thick" questions, is easier to remember and reproduce. Students are trained to work independently on the content of an article or work. Reading becomes thoughtful, mindful.

The laboratory workshop was built on the technology of problem-based learning. Such an organization of training sessions, which involves the

creation of problem situations (cases) under the guidance of a teacher and active independent activity of students to resolve them, contributes to the development of creative mastery of knowledge, skills, abilities and the development of thinking abilities. The goal is to promote the development of students' problem thinking, their ability to evaluate information qualitatively and objectively.

Also, as part of the study of the discipline, future bachelors in the field of applied computer science participate in the educational and research project "Classification of threats in the subject area".

The project method is considered one of the leading in the bilding of students' speech competencies, the ability to use a foreign language as a tool for intercultural communication and interaction. Project work is one of the forms of organizing the research cognitive activity of students, in which they take an active subjective position. The topic of the project is directly related to the building competencies in the information security field and the professional field of future bachelors of applied computer science (Chernova E.V., 2015).

4 DISCUSSION

So, we have identified the descriptors of competencies that, in our opinion, should be built as a result of studying the discipline "Information security". Although the bachelor of Applied computer science will not perform the same job functions as information security specialists, their training should be sufficient to enable them to design and build secure and reliable information systems. The main task of teachers, in our opinion, is to maintain a balance between the volume and sufficiency (simple and complex) of educational material, and we believe that the proposed solution will solve it quite well. Of course, the proposed concept is a scheme, which in the future will be supplemented by methods, tasks, examples of which we have given above. The pedagogical search is not complete, but it has found the necessary boundaries, the kind of centers of crystallization around which the academic discipline is built.

5 CONCLUSIONS

Based on the conducted research, it can be concluded that the training of specialists in the information security field is an urgent task of modern society, the solution of which is tied to the scientific justification and identification of the complex of necessary competencies that a modern specialist should possess. The components of competencies in the information security field identified by us, the generalized tabular model of these competencies proposed by us, as well as the stages, methods and forms of building these competencies in bachelors of Applied computer science on the example of APC-2, require additional study. The conducted research allows us to outline ways to solve the multifaceted and complex problem of building students' competencies in the information security field, taking into account modern requirements for training specialists not only in the field of computer science and information technology.

REFERENCES

Chernova, E. V., Gavrilova, I. V., Romanova, M.V. and Dokolin A.S. (2017) Information Technology in Business Continuity. In *Proceedings of the IV International research conference "Information technologies in Science, Management, Social sphere and Medicine" (ITSMSSM 2017)*, pages 283-286. doi: 10.2991/itsmssm-17.2017.58

Chernova, E.V. (2015) Innovative educational technologies in teaching the basics of information security. *Electrotechnical Systems and Complexes,* 1 (26), 52-55.

Chernova, E. V. (2019). *Practical course on Information security for Bachelor of Applied Informatics*. Magnitogorsk: NMSTU.

Chomsky, N. (1972) *Aspects of the theory of syntax*. M., MSU Publishing House.

Choshanov, M.A. (1996). *Flexible technology of problem-based modular training.* Moscow: Narodnoe obrazovanie (Public education).

Chusavitina, G.N., Zerkina, N.N. and Makashova V. N. (2018). Special aspects of future teachers' training in ensuring information security sphere for university students. *Perspectives of Science and Education*, 35 (5): 259-266. doi: 10.32744/pse.2018.5.29.

Federal State Educational Standard of Higher Education Level of higher education Bachelor's degree course of study 09.03.03 Applied Informatics. http://fgosvo.ru/uploadfiles/fgosvob/090303.pdf

Federal State Educational Standard of higher Education-Bachelor's degree in the field of training 09.03.03 Applied Informatics. Retrieved from: http://fgosvo.ru/uploadfiles/FGOS VO 3++/Bak/090303_B

Federal State educational standard of higher professional education in the field of training 230700 Applied Informatics (qualification (degree) "bachelor"). http://fgosvo.ru/uploadfiles/fgos/22/20111115155948.pdf

Gavrilova, I.V. (2017). *Fundamentals of evaluating the effectiveness of IT projects.* Magnitogorsk: NMSTU.

Gorbunov, A.I. (2012). *Building professional competence in the field of information security for future economists in the context of higher education*. (Doctoral dissertation) Mari State University. Cheboksary.

Khutorskoy, A.V. (2003). Key competencies as a component of the personality-oriented paradigm of education. *Narodnoe obrazovanie (Public education)*, 2(13325), 58-64.

Postupi.Online (2021). List of universities where you can get the profession of a Specialist in applied computer science. https://postupi.online/professiya/specialist-po-prikl.

Troyanskaya, S. L. (2016) *Fundamentals of the competence approach in higher education: a textbook.* Izhevsk: Publishing Center "Udmurt University".

Zakharov, S. Yu. (2019) Personnel as a factor of enterprise competitiveness. In *Actual issues of economics and management: materials of the International Scientific and Practical Conference,* Magnitogorsk. 48-51.