

# Experience in the Formation of Competencies in the Field of Information Technology Security in the Educational Programs of MIEM NRU HSE

*Aleksandr Belov*<sup>1\*</sup>, *Artem Kabanov*<sup>1</sup>, and *Alexey Los*<sup>1</sup>

<sup>1</sup>National Research University Higher School of Economics, Moscow, 123458, Russia

**Abstract.** The paper discusses the development and testing of a model of competencies in information security which ensures the effective interaction of society, business, the labor market and education in the digital economy. The proposed model is based on the requirements of employers for the training of a modern engineer. In accordance with the developed competency model in the field of information security the original educational standards for engineering education implemented at MIEM NRU HSE were modernized.

## 1 Introduction

Digital technology is booming all over the world. More and more areas of the economy are using the capabilities of technologies such as Internet of Things, artificial intelligence, data analysis, virtual reality, etc. The digital transformation of the economy involves the introduction of modern technology in the business processes of the enterprise [1]. The concept of smart manufacturing based on the industrial Internet, combining physical production and operations with intelligent digital technologies, introduces fundamental changes in management approaches, corporate culture, external communications [2] as well as the key competencies of a modern engineer [3-5].

Obviously for the successful implementation of the digital technologies it is necessary to make significant changes both in the educational programs for training engineers and in approaches to their implementation with the aim of developing skills in such areas as: big data analysis technologies, industrial Internet, cyber-physical systems, cloud technologies for storing and processing information, etc. [6 - 8]. Cybersecurity occupies a special place in this series.

The issues of ensuring data security, the security of information systems and technologies themselves ensuring safe information interaction between people and business in the digital economy are becoming extremely important for the digital transformation of the state and society [9 - 13]. It is this circumstance that explains the need to form competencies in the field of information security among engineering personnel. Modern production companies and enterprises are in dire need not only of specialists in cybersecurity, but also of engineering and technical workers with the necessary skills in the

---

\* Corresponding author: [avbelov@hse.ru](mailto:avbelov@hse.ru)

field of information security a high level of cyber hygiene and cyber culture [14]. All this leads to the need to review the content of educational programs in engineering universities, the formation of a model of professional competencies in the field of information security.

## **2 The requirements of employers for the training of engineers in the field of information security**

In accordance with the approach adopted by the Moscow Institute of Electronics and Mathematics National Research University Higher School of Economics (MIEM NRU HSE) formulated in the standards of the CDIO Worldwide Initiative [15] constant feedback from industrial partners has been implemented to analyze the requirements of employers for the competencies of graduates of educational programs to take into account current trends in engineering training. Representatives of employing companies are members of the Academic Councils of Educational Programs, expert commissions when conducting project sessions and defending projects carried out by students of MIEM NRU HSE. In particular the Academic Council of the Computer Security Education Program includes representatives of law enforcement agencies and representatives of the Cyber Security Department of Sberbank of the Russian Federation of maturity and continues to develop.

Representatives of these organizations participate both in the preparation of curricula of the educational program of the KB, the formation of programs of academic disciplines and directly in the implementation of the educational process: they conduct classes in a number of disciplines of the professional cycle, manage project activities, internships, term papers and dissertations.

Programme Academic Supervisors of educational programs and members of the Academic Council regularly conduct surveys of employers in order to obtain information on how they evaluate the professional training of students which competencies need to be developed at the moment and which will be in demand in the near future. As a result of the surveys in addition to solid basic knowledge of mathematics, programming and other technical disciplines the following requirements for the competencies of engineering graduates were formed [16]:

1. knowledge of applied methods, tools for solving practical problems,
2. the ability to correctly understand the content of the task,
3. skills to work in team,
4. cyber security skills,
5. the ability to find and correctly use information from various sources to solve professional problems,
6. the ability to master new areas of knowledge and skills,
7. the ability to comply with deadlines,
8. the ability to correctly present the results of the work performed.

According to 80% of employers participating in surveys the most important are the competencies: 1 – 4, which indicates that during the period of digital transformation soft skills and knowledge in the fundamental mathematics, physics, IT and cyber securities are most in demand.

## **3 The curriculum competency model " Computer security"**

As a result of mastering the educational program a graduate of the Higher School of Economics will form universal and professional competencies. The totality of all competencies formed by the graduate ensures his ability to carry out professional activities

in at least one area or field of professional activity, or to solve the tasks of professional activity of at least one type established in the HSE original educational standard [17].

Professional competencies are determined on the basis of professional standards corresponding to the professional activities of graduates as well as on the basis of an analysis of labor market requirements, generalization of foreign experience, consultations with leading employers, associations of employers in the industry in which graduates are in demand [18].

The main professional competencies that a graduate of the Computer Security educational program should have can be presented in the form of a Table 1. This table is called the competency model.

**Table 1.** Competency Model

<b>№</b>	<b>Competency Statement</b>
1	The ability to protect information in the computer and computer networks.
2	The ability to protect operating systems
3	The ability to protect information in database management systems
4	The ability to provide technical, antivirus, cryptographic protection of information in computer systems
5	The ability to develop computer system security models
6	The ability to analyze the security models of computer systems, including compliance with domestic and foreign standards in the field of computer security
7	The ability to apply mathematical methods to assess the security of computer systems including by designing their mathematical models
8	The ability to develop design and technical (including reporting) documentation
9	The ability to develop draft regulatory legal and methodological documents in the field of information security
10	The ability to analyze design decisions to ensure the security of computer systems
11	The ability to make an informed choice of software and hardware implementations of information protection methods

As can be seen from Table 1 very serious requirements are imposed on the graduates of the educational program “Computer Security” both in terms of directly ensuring the security of computer systems and networks and in terms of analyzing and justifying the level of security of these systems. And related design decisions as well as parts of the preparation of the necessary supporting documentation.

#### **4 The implementation of a competencies model in the field of information security in the engineering educational programs**

The issue of designing the necessary competencies in students has two sides: the first side is the direct formation of these competencies, the second is the establishment of the fact of their presence that is the establishment of the availability of necessary knowledge, skills.

In order to solve these problems, a detailed analysis of the problems of training engineering personnel in the field of information protection and the formation of basic professional competencies was carried out at MIEM NRU HSE. Such acute problems of

training modern engineers as the low level of cyber hygiene and cyber culture, the insufficiently high and often one-sided level of training of specialists in information protection, and the acute shortage of these specialists in the labor market are noted. Based on an analysis of already existing experience in training information security specialists as well as an analysis of the needs of partner organizations of MIEM NRU HSE especially those at risk and subject to regular cyber attacks methods are proposed for building the competencies required for these specialists to work in the digital economy and a methodology verification of their implementation. The proposed competency model is being tested including project activities in the interests of industrial partners, internships, participation in competitions in the profile of training and involvement of employees of partner organizations in the formation of the necessary competencies and assessment of the level of students' training.

Table 2 shows the names of a number of partner organizations of the “Computer Security” educational program and their areas of information protection. Every year, students of the educational program undergo practical training and internships in these organizations under the direct supervision of leading specialists who help students in the formation of the necessary skills, thereby forming the required competencies.

**Table 2.** The industrial partners in the cyber security

<b>№</b>	<b>Industrial Partner</b>	<b>Information security field</b>
1	Department of Cybersecurity of the Sberbank of the Russian Federation	Combating fraud and cybercrime
2	The company "Contech"	Development of software for information security, information security management
3	Kaspersky Lab Security	Incident Analysis, antivirus software development
4	Company "Active"	Development of software and hardware for providing information security
5	LLC “Inoventika”	Remote traffic analysis, detection of computer attacks
6	GRAND TORTON	Information Security audit, development and implementation of penetration tests
7	Company “Gamma”	Development and testing of applications for cryptographic and technical information protection
8	Company “InfoWatch”	Protection against an internal intruder

Directly communicating with students in the process of solving production problems, representatives of partner organizations get an idea of the students having the necessary knowledge and skills, their abilities to master new questions and problems for them, the ability to independently find solutions to problems, and the ability to work in a team. Representatives of the industrial partners reflect their opinion on all these issues including the availability of the necessary competencies in a detailed report on internships which is one of the required indicators for the formation of competencies.

An important element in the implementation of the considered competency designing model is the participation of students in project activities [18]. Table 3 is presented some topics of projects in which students of the educational program “Computer Security” participated in the 2018-2019 academic year and their types.

**Table 3.** Student Project Topics

<b>№</b>	<b>Project name</b>	<b>Project Type (Research/ Practice oriented )</b>	<b>Command Project/Individual Project</b>
1	Development of a universal tool for tunneling TCP traffic through the DNS protocol	Research Project	Command Project
2	Studying of technical measures to protect network applications from the imposition of information	Research Project	Individual Project
3	Development of simulators of information retrieval devices to demonstrate the operation of the indicator of the “Catcher” field	Practice oriented	Command Project
4	Finding Usable IPv6 Addresses Using NTP	Practice oriented	Individual Project
5	Development of a time-based user-space filter system assignments	Practice oriented	Individual Project
6	Designing a Corporate Network Lab in Cisco Packet Tracer	Practice oriented	Individual Project
7	Creating an assistant system for conducting online classes	Practice oriented	Individual Project
8	Conducting an audit of vulnerabilities of the external perimeter of the University	Practice oriented	Command Project
9	Development of tools for detecting fraudulent transactions with bank cards of individuals	Practice oriented	Command Project

As can be seen from Table 3 the topics of projects carried out by students of the design bureau and their types are very diverse. The project implementation procedure consists of two stages. At the first stage students choose topics, make up a detailed technical task and shoot a short video with a presentation of the task. At the second stage direct substantive work is carried out to fulfill the technical specifications. At the final stage students draw up a detailed report on the work done and a short presentation that they make before the examination committee. The assessment for the project consists of the assessment of the first and second stages including the assessment for the presentation and assessment of the project manager [19].

An important tool for the formation of the necessary competencies is the activity of students performed in the process of passing various kinds of internships. This type of study forms the student’s competencies allowing to solve the practical problems of the chosen profession including design, research, entrepreneurial, expert and analytical activities.

The curriculum of the Computer Security educational program provides for three groups of internships:

- the internships in the companies and organizations or in the workplace;
- the design internships;
- the research internships.

The following methods of conducting internships are allowed: stationary and visiting.

A group of internships in the companies or organizations or in the workplace includes educational, industrial and other types of internships. The group of design internships includes: student's project activities (project, course project), project seminar as mentioned above.

The group of research internships is including: the preparation of the thesis, written coursework of a research nature, a research seminar (RS).

RS is provided for a limited circle of students who have chosen the research or expert-analytical option as the main type of future professional activity. Both the University employees and invited specialists with experience and significant achievements in the field to which the scientific seminar is oriented are involved in the RS.

Currently studies to test the above competency model are ongoing in the search for new forms of their formation and verification of content. In particular, discussions are being held to address the issue of accounting in determining the level of formation of competencies of individual and group achievements of students in scientific work helping teachers to conduct the educational process and various competitions in the profile of training, such as CTF and several others.

As noted above the second important point in the formation of student's competencies is to establish the fact of their presence that is to establish the availability of the necessary knowledge, skills and abilities both in the field of natural Sciences and in the professional field.

Traditional methods of testing student's knowledge and skills are various forms of intermediate and final control, determined by the leading subject teacher. The intermediate forms of control usually include colloquiums, control and independent work, homework and laboratory work, presentation of reports and abstracts on the subjects studied. The forms of final control usually include tests and exams which in turn are written and oral as well as in the form of computer tests.

The final control in the disciplines of natural science cycle such as mathematics, physics, information theory as a rule is carried out in the form of an oral exam in which students receive tickets containing theoretical questions and problems. In the theoretical part at the same time it is required to prove some statement and to solve the problem in any known way and explain the course of the solution. A convenient form of final control is a combination of written and oral examination when first the teacher is given a written task and checked its implementation and then an oral interview is conducted.

When determining the final grade on the subject along with the assessment for the exam, the results of the intermediate control are also taken into account. This approach on the one hand stimulates continuous work during the period of study of the discipline and on the other allows you to more objectively assess the development of the stated competencies [20].

Modern information technologies make it possible to apply other forms of intermediate and final control of the development of competencies especially in the professional field. An example of such forms of control are computer business games in which the student must perform various tasks: to find vulnerabilities, identify malicious impacts and neutralize them, to develop a system of protection of a local, remote network or database, to detect traces of a computer attack and other similar tasks. In the course of these tasks the teacher or the Commission is not difficult to make an objective conclusion about the level of development of the relevant competencies of the student.

It seems that the problem of constant search and introduction of modern methods and technologies both in terms of the formation of competencies and in terms of checking the level of their development is very important in the issues under consideration.

As an illustrative example of modern technical means of training let us consider a training stand that simulates the operation of an automatic process control system (ACS) [21].

The stand consists of the following main parts:

- Models of three enterprises in respect of which the attack on the ACS TP can cause serious damage: power plant, oil pumping station, railway,

- The Cisco Catalyst 2960 Switch,
- Layout controls,
- Administrator computer,
- The attacker's computer.

The photo of the stand is shown in Figure 1.



**Fig. 1.** General photo of the studied stand

As noted above the stand has three main modes (scenarios) of operation:

1. Layout of the power plant, the administrator works with the power plant management console.
2. Layout of the oil pumping station, the administrator works with the control console of the oil pumping station.
3. Layout of the railway, the administrator works with the power grid management console.

Work on the stand involves the actions of an attacker trying to use specially implemented vulnerabilities, to carry out unauthorized access to process management in order to change the normal mode of operation of the enterprise. The actions of an information system security officer involve the detection of an intruder's interference and its neutralization. The student performing the role of an attacker demonstrates the ability to find and exploit system vulnerabilities, and the student performing the role of a security officer demonstrates the ability to detect the intruder and eliminate the consequences of his activities.

Work at this stand is a business game and serves as an objective test of the knowledge and skills gained in terms of ensuring the security of real information systems.

## 5 Conclusion

The proposed competency model in the field of information security was used in the development of original educational standards for engineering training programs at MIEM NRU HSE. It took into account the requirements of industrial partners as well as modern technologies of digital education.

## References

1. C. Matt, T. Hess & A. Benlian, *Digital Transformation Strategies*, Bus Inf Syst Eng 57, pp. 339–343 (2015) doi:10.1007/s12599-015-0401-5/
2. Jung, Kiwook *Mapping Strategic Goals and Operational Performance Metrics for Smart Manufacturing Systems*, in Procedia Computer Science, **44**, March 16 2015, pp. 184–193 (2015). doi:10.1016/j.procs.2015.03.051
3. V.P. Soloviev, T.A. Pereskokova, *Technical education in Russia: problems, ways of solution*, in Engineering Education, **no. 24**, pp. 30–40, Russia (2018)
4. F. Smulders, A. Kamp and C. Fortin, *The CDIO framework and new perspectives on technological innovation*, Proceedings of the 14th International CDIO Conference, in Kanazawa Institute of Technology Kanazawa (Japan), June 28 – July 2, pp. 40–52 (2018)
5. V.G. Ivanov, A.A. Kaybiyaynen, L.T. Miftakhutdinova, *Engineering Education in Digital World*, in Higher Education in Russia, **No. 12 (218)**, pp. 136-143, Russia (2017)
6. Yang, Chen; Shen, Weiming; Wang, Xianbin , *The Internet of Things in Manufacturing: Key Issues and Potential Applications*, IEEE Systems, Man, and Cybernetics Magazine, **4 (1)**, pp. 6–15, January 2018, (2018) doi:10.1109/MSMC.2017.2702391
7. A. Los A., V. Semin, A. S. Kabanov, E. R. Khakimullin, *Problems of Information Security Technology the "Internet of Things"*, in Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS). IEEE, pp. 110-113 (2017)
8. V. Kupriyanovsky, V. Sukholmilin, A. Dobrynin, A. Raikov, F. Shkurov, V. Drozhzhinov, N. Fedorova, D. Namiot, *Skills in the Digital Economy and the Challenges of the Education System*, in International Journal of Open Information Technologies, **No. 1**, pp. 19-25, Russia (2017)
9. Work in the automation age: sustainable careers today and into the future [Electronic resource]. Association for Advancing Automation, Ann Arbor, April 2017. – URL: <https://www.a3automate.org/docs/Work-in-the-Automation-Age-White-Paper.pdf> (accessed: 14.12.2019)
10. Skills for a Digital World. Policy Brief on The Future of Work [Electronic resource] // OECD. – 2016. – URL: <http://www.oecd.org/els/emp/Skills-for-a-Digital-World.pdf> (accessed: 21.02.2018).
11. The Digital Competence Framework for citizens. URL: <https://ec.europa.eu/jrc/en/digcomp/digitalcompetence-framework> (date of issue 12.02.2019)
12. D.E. Goldberg, *The Missing Basics and other Philosophical Reflections for the Transformation of Engineering Education. Excerpt from "What engineers don't learn and why they don't learn it: and how philosophy might be able to help"*, in Abstracts of the 2008 Workshop on Philosophy and Engineering, pp. 85-86 (2008)
13. A. Kamp and R. Klaassen, *Impact of global forces and empowering situations on engineering education in 2030*, in Proceedings of the 12th International CDIO Conference, Turku University of Applied Sciences, Turku, Finland, June (2016)
14. ECDL Foundation. Skills for Data Protection. URL: <https://icdl.sharefile.com/share/view/sc570cbe144e4052b> (date of issue 12.02.2019)
15. Kristina Edström & Anette Kolmos, *PBL and CDIO: complementary models for engineering education development*, in European Journal of Engineering Education, **39:5**, pp. 539-555, (2014) DOI: 10.1080/03043797.2014.895703

16. A.V. Belov, A.V. Serova, *Designing a Bachelor's curriculum model "Applied Mathematics" based on international standards of engineering education*, in Proceedings of the I All-Russian Scientific Conference "Layered training specialists: e-learning and open educational resources", Tomsk Polytechnic University. – Tomsk: Publishing house of Tomsk Polytechnic University, pp.390- 392 (2014)
17. The HSE Educational Standard in Computer Security. URL: <https://www.hse.ru/ba/cosec/documents> (accessed: 14.12. 2019)
18. S.E. Tsvetkova, I.A. Malinina, *Designing of vocational training for engineers in the context of competency-based approach. Engineering Education*, **no. 23**, pp. 33–44, Russia (2018)
19. A.V. Belov, T.I. Soloveva, A. Vnukov. *Complex education program "Project Seminar" to meet today and tomorrow needs of fast developing optical-electronic industry*, in: ISSE 2017 40th International Spring Seminar on Electronics Technology. Red Hook: IEEE Computer Society, pp. 1-7 (2017)doi 10.1109/ISSE.2017.8001001
20. A.V. Belov, A. B. Los, Experience in organizing project training at the Computer Security educational program at HSE MIEM, in the collection: ACTUAL PROBLEMS OF ENSURING INFORMATION SECURITY Proceedings of the Interuniversity scientific-practical conference, pp. 53-59 (2017)
21. A.S. Kabanov, Yu.I. Gudkov, V.N. Azarov. *Problems and Prospects of Security in the Transport Sector*, in Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS). IEEE, pp. 132-135 (2019)