Social Work
& Education

©SW&E,2017

Voskoboinicov, S. &. Melnyk, S. (2018). Cyber security in the modern sociation and improvement of preparation of future factors in the field of competent approach, *Social Work and Education*, Vol. 5, No. 1., pp. 103-112.

CYBER SECURITY IN THE MODERN SOCIATION AND IMPROVEMENT OF PREPARATION OF FUTURE FACTORS IN THE FIELD OF COMPETENT APPROACH

Sergiy Voskoboinicov,
PhD, Senior Lecturer,
Educational and Scientific Institute of Information Security National Academy of Security Service of Ukraine,
Kyev, Ukraine,
s_voskoboynikov@ukr.net

Сергій Воскобойніков,
кандидат педагогічних наук,
старший викладач,
Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України,
Київ, Україна

Sergiy Melnyk,
PhD, associate professor,
Educational and Scientific Institute of Information Security National Academy of Security Service of Ukraine,
Kyev, Ukraine

Сергій Мельник,
кандидат технічних наук, доцент
Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України,
Київ, Україна

УДК 378:004.023:004.056.53

DOI:10.25128/2520-6230.18.1.10

Article history:
Received: Febuary 28, 2018
1st Revision: March 20, 2018
Accepted: March 31, 2018

Abstract. Trends in the development of higher professional education in the conditions of the information society confirm its transformation in accordance with the expansion of the spheres of professional activity and education related to the significant dynamics of the development of the information component of human life and society. The state of the development of the information society and information infrastructure of Ukraine determines the professional requirements of public and private structures for the training of specialists in the field of information security and information-psychological confrontation of technical, humanitarian and economic specializations. These areas of professional activity have been developing significantly in the last three decades, and the sphere of cyber security since the 2000 (with the notion of the national system of cyber security in Ukraine legally determined only in 2016). The content of the concept of cybersecurity covers not only technology, but above all human resource. Today, the majority of representatives of agencies involved in the national system of cyber security of Ukraine, note the urgency and the need for proper staffing by professionals of the relevant specialization.

Theoretical analysis, generalization and definition of the role of cyber security in modern society and training of future specialists of the branch in higher educational institutions, tendencies of modernization for organization of educational processes on the basis of competence approach, system analysis of legislative, normative and regulatory basis, pedagogical experience of professional training of future cybersecurity specialists in higher education institutions.

The scientific and technological revolution has caused deep system transformations around the world. First of all, due to the improvement of achievements in the field of the latest information technologies with the assets that arose on the basis of the rapid development of information and telecommunication systems, fundamentally new comprehensive issues – the information society, as well as informational and cybernetic spaces, which today cover virtually unlimited potential and play a leading role, have been formed, role in the economic and social development of each country in the world

Keywords. Cyber Security, information society; IT- technologies; higher professional education; future professional activity; competent approach.

Introduction

At the present stage of development of science and technology, cybersecurity of each developed state turns into one of the most important branches of high-tech society. Due to the widespread use of modern information technologies in all spheres of its existence, society has become vulnerable to insignificant cybernetic influences that increasingly become an effective tool for achieving the goal of non-controlling control and management as objects of critical infrastructure of the state, enterprises and individual citizens, their associations. The streams of information being transmitted, stored and processed in cyberspace are constantly increasing, requiring their proper protection against unauthorized access with a criminal purpose. Therefore, the need for specialists in cybersecurity is relevant and with the further development of high-tech society will increase even more. The training of specialists in cybersecurity requires the proper technological equipment of the higher educational institution, attracting highly qualified specialists. In the preparation of this kind of specialists interested enterprises and organizations of Ukraine. According to B. Bystrova, the effectiveness of their preparation is associated with the reform of the higher education system in Ukraine at all levels, which is aimed at creating a flexible system of access to continuing education, and the development of perspective models of training highly skilled, competitive information professionals' technologies, cybersecurity in accordance with world standards (Bystrova B. V., 2017, 22–24).

The design of educational standards for the training of cyber security specialists for drafters is fundamentally new, notes I. Dioritsa, since: the specialty was introduced for the first time, and therefore, as a sample can serve only foreign experience; The Law of Ukraine "On Higher Education" of 01.07.2014 introduced fundamental changes regarding the content of the standardization of education and the accompanying processes. The educational standard is defined as a set of requirements for the content and results of educational activities of higher educational establishments and scientific institutions at each level of higher education within each specialty (Dioritsa I., 2017, 50–53).

Analyzing the best practices in the field of Cyber Security at the US universities, it should be noted that the educational process combines the theory and know-how of evaluating, planning, designing and implementing effective cybersecurity measures in the public and private sectors, focused on the career of specialists from digital (computer, IT) criminologists, cyber security analysts and consultants. The training programs meet the requirements of the 8570.01-M of the US Department of Defense (American Military University official site, 2016; Information Assurance Workforce Improvement Program Department of Defense ...., 2016) and the objectives of the International Association of Computer Experts (IACIS) (Mel'nyk S., Voskoboynikov S., 2016, 328–345; Information Assurance and Security Education Center .., 2016).

The modernization of the higher education system for the preparation of bachelors on cybersecurity provides the following results: a) after 2 courses the English language - B2; b) the development of "Soft Skills" that can be successful regardless of the specifics of the activity (persuasion skills, people's attitude to work, teamwork, characteristics: erudition, creative thinking, leadership, negotiation skills, language proficiency, work with information);) all preparatory disciplines are subject to professional and are taught at 1-2 courses; d) on the 3-4th year of vocational training through dual education and free access to the online platform of the mixed type of training; e) the training program is subject to the requirements of international certification programs CISSP, ISACA and typical job descriptions of the leading companies of the world, generalizes the results of foreign experience B. Bystrova (Bystrova B. V., 2017, 22–24). At the same time, in Ukraine, with the training of specialists in cybersecurity revealed real problems: the unpreparedness of graduates to take international professional exams and work on a specialty; lack of practical communication skills among graduates.

To date, according to B. Bystrova, there is a need for in-depth analysis of integration processes in various fields of information security, in particular cybersecurity, in connection with the development of the IT industry and its penetration into key components of professional activity and components of the educational environment itself higher education institutions. In addition, innovative developments in the direction of intellectualization of professional tools of a cybersecurity expert are rapidly developing, which inevitably makes us think about the need to include in the educational environment the infrastructure components of student innovation development and its impact on the modernization of the educational process (Bystrova B. V., 2017, 15–18).

Cybersecurity (formerly "Security of Information and Communications Systems") is an in-depth study of approaches and methods for developing and administering software and hardware information security solutions that solve information security tasks in cybernetic space. According to the current demands of the society, the qualification characteristic of specialists of specialty 125 "Cyber Security" should provide: competence and ability at the technological level - development and introduction of productive, reliable and virus-resistant software fragmentation; secure networked channels; protected databases, to which it is impossible to add stunned information, unauthorized reading of confidential data, means of detecting and disposing of damage, monitoring information security; operating systems protected from internal and external attackers; Web servers that are resistant to network attacks, comprehensive information security systems that counteract the many and varied nature of threats (cyberattacks by insiders and hackers, software frauds, viruses, interception of traffic, information attacks, wars, mistakes, information leaks, international terrorism); At the managerial level – the creation of a system of information and cyber security in the structure of the enterprise, organization and at the state level.

Today, in the framework of the state program of modernization of educational standard in the direction of "Cyber Security", methodical recommendations for the preparation of educational materials have been developed; the structure of preparatory disciplines is formed; the work on preparation of curricula for the 1-2 courses (2017-19 years) and preparation of educational materials for preparatory disciplines has been started; A round table was held at the Ministry of Education and Science of Ukraine with leading universities; It is planned to make free access to the online platform of the mixed type of training; Create a community of cyber security lecturers and experts. Higher educational institutions have already joined the project. The emphasis is placed on increasing confidence in Ukrainian higher education institutions, which are training specialists in the field of information security, cyber security from employers and entrants (Bystrova B. V., 2017, 22–24; Dioritsa I., 2017, 50–53).

Discussion

The formation of a competent responsible specialist for the field of cyber security is a priority benchmark in the system of modern higher education in Ukraine. The formation structure in the organization of the system of professional training of future specialists in cyber security in higher educational institutions is motivational, epistemological, phraseological, informational and technological, monitoring and evaluative-reflexive components. On the basis of the results of the system analysis of the experience of improving the system of professional training of specialists in higher educational establishments, we determine that in today's conditions, a combination of activity and competence approaches is effective. Activity approach involves the use of active learning methods that allow students to develop thinking, use the knowledge gained in practically oriented activities, which is as close as possible to professional. At the same time, it is extremely important to evaluate not only knowledge and skills, but also the creative autonomy, information and technology aspect of the maintenance of the educational process. Competent approach also determines the use of a special methodology taking into account the sector specifics of training, professional activities, the essence and content of professional orientation of vocational training in accordance with the needs of society (Mel'nyk S, 2016).

Therefore, modernization of educational processes in the system of professional training of future specialists in cybersecurity, taking into account the specifics of their future professional activities in accordance with the specialization of the activities of training, we consider through the prism of the formation of professional competence in accordance with modern societal demands.

The modern branch of information and cyber security activities includes legal, organizational, technical and law enforcement components, concerning information and technological and information-psychological confrontation. At the same time, the bulk of the modern labor market is determined by the needs of specialists in technical and cryptographic information security in cyberspace (hereinafter - information security).

The terms "technical" and "cryptographic protection of information" are regulated and widely used in the professional environment. In the United States of America and the European Union, terms such as "information security" in the sense of information security, "cyber security", "IT security", "computer and network computer and network security", "computer system security", "information system security", "electromagnetic information security", "physical information security", "information security)", "information security management", "cryptography (cryptography) and others (Mel'nyk S, 2016).

Considering the protection of information as a component of information security, we will focus on the fact that in the normatively fixed terms in Ukraine, modern information security activities include consideration of: legal issues of determining the necessity and order of information protection, legal support for the stages of development, implementation, operation and decommissioning systems of protection; technological issues of information security in information and telecommunication systems and objects of information activity; organizational and technical issues of information security management (or rather, management of information protection). Taking into account the social necessity and social order for the training of future specialists in the protection of information, as well as the essence of professional activity, consider the mentioned problem in the context of modernization of the content and forms of educational process for the training of future specialists in the field of cyber security on the basis of a competent approach.

Summarizing the results of the study of the competent approach of the US Institutes of Higher Education, one can distinguish the main feature – the "flexibility" of the educational process, focused on the success of each student in the formation of professional competence, accessibility of higher education, in particular. This "flexibility" consists in the formation of a personal curriculum, that is, a graphic study of academic disciplines, taking into account personal intellectual capabilities, results of prior learning, existing experience, professional inclinations and preferences. At the same time, the number of normative disciplines in the leading higher educational institutions is significantly lower compared to the student's choice of disciplines, which allows each individual to plan his own system of education and professional development and continuous lifelong learning more effectively.

Additionally, in the higher educational institutions a scheme of individual mentoring (Student Mentor) is implemented - assistance provided to the student of the contact person in planning and correcting the organization of training on an individual trajectory, taking into account the results of vocational guidance and wishes of the student regarding the distribution of his physical and mental load - providing his own comfort while studying.

The proven time of innovation is also the on-line learning (e-learning) of information security professionals within the bachelors and master's programs, as well as postgraduate education. Apparently online training only in conjunction with the outlined peculiarities of competence and personality-oriented approaches provides the basis for a real increase in the availability of quality education for future and current professionals in the protection of information and professional development.

The Master's program in Cyber Iecurity of Information Services focuses on future private sector digital economists with key competencies in line with the 2014 NATIONAL National Security Initiative (NICE) for Workforce Framework (NICE official site, 2016).

The main thematic areas of professional training are: "risk management", "cyberwarfare", "law enforcement of cyber security", "security policy", "hardware and software security", "ethical hacking", "criminalistics of network intruders (comp "Computer or IT criminology"), "Emergency recovery, prevention and response".

Of particular importance in the system of masters training in the specialty "Cyber Security" at the American Military University is to use a broad interdisciplinary approach to preventing and responding to large-scale cyber threats and cyber-attacks. The first half of the study program includes the foundations of network security, cybercrime and digital criminology. The second half of the program focuses on policies, practices and prospects for cybersecurity within national security, intelligence, criminal justice and emergency management. The main thematic areas of the disciplines of professional training are "perspectives of emergency management and cyber security", "management of security risks by methods of prevention of losses", "history, development and efficiency of cyber intelligence", "computer (digital, IT) forensics: tools, procedures and legislation", "prevention and investigation of cybercrime", "telecommunications and network security: prevention, detection and response to incidents", "cyber-laws, ethics, intellectual property and criminal prosecution".

The MSc "National Security" and "Internal Security" provide for the consideration of individual issues of information security within an integrated approach to ensuring national and internal security.

The peculiarity of on-line training at the American Military University is the integrated approach to the professional training of specialists in information and cyber security of the public and private sectors in terms of providing public, internal, national and international security, as well as the use of state and community access programs for higher education of military personnel. and veterans (free tuition or discounts for educational services for servicemen, veterans and students who have decided to sign You are contracting with the Ministry of Defense (DOD), the National Security Agency (NSA) and the United States DHS.

On the basis of the carried out analysis it is possible to systematize the thematic filling of the bachelor program of future specialists in the field of information protection, consisting primarily of such professional orientations as: "Architecture and models of security"; "Data security"; "Security of IT operations"; "Protection of operating systems"; "Computer security"; "Network security"; "Network security management"; "cryptography"; "Physical information security"; "Information security risk management"; "Ensuring business continuity and recovery from failures"; "Audit of information security"; "IT Law and Ethics"; "Cyber legitimacy and privacy of privacy in the era of digital technologies." In turn, the thematic content of the master's program of future information security professionals includes, above all, the competence to develop security policies, the development and operation of protection technologies at different levels of the OSI model, and the processing of information security incidents. It is necessary to summarize that the legal and economic components of professional competence of future specialists in cybersecurity are formed by special disciplines in specialties in the process of master's training in legal, economic and technical sciences.

As for the modernization and introduction of new forms of organizing the educational process for the training of future specialists in the field of cybersecurity, it is necessary to distinguish between interactive methods and forms of holding classroom and distance learning to improve the conditions for students to perform their independent work.

To improve the organization of the professional training of future cyber security specialists, we recommend using heuristic methods for solving problems in the system of student competence training.

In the process of introducing a competency approach in the higher education system there is an increasing role of competency-oriented forms: interactive forms of learning, problem-based training in groups, special training sessions for active group training in professional and communicative aspects. Currently, new forms of education are being implemented on the basis of a competent approach, the transition from passive perception of information to the methods of active information learning, effective learning of learning material on the basis of active management of cognitive activity of students, the development of their cognitive interest in the study of special educational disciplines, the formation of future specialists readiness for realization of professional competences in practical activity.

The basic direction of solving these tasks is the transition from explanatory-illustrative to active teaching methods, which increase the effectiveness of learning not by increasing the amount of information, but by improving the efficiency of its processing, form the necessary professional qualities on the basis of preparedness for the implementation of professional competences in the future specialists in information security, motivation for further enhancement of professional skills, professional creative development.

The professional activity of a specialist in the protection of information requires not only understanding, memorizing and reproducing the knowledge gained, but also the most important thing – their ability to operate, effectively apply – to act promptly in non-standard conditions in future professional activities and to creatively develop their professional qualities. The achievement of this goal is promoted by active teaching methods, aimed at the development of students, creative independent thinking and the ability to professionally solve professional problems. The use of these methods ensures not only the activation of creative educational activities, but also the close connection between theory and practice. In the process of problem learning, we used heuristic methods in the business game "Cybersecurity Risk Management", on the basis of which students independently work out algorithms for managing cybersecurity in solving problem situations, as closely as possible future professional activities.

Conclusions

The trends of modernization of the professional training of future cybersecurity specialists include: the creation of new technologies in accordance with the world level of IT technologies development, new spheres, specialization in professional activities, and ensured by the technological, managerial levels of professional activities for ensuring cyber security in society, the state and its citizens, international cooperation and industry for IT support and security of electronic document management using local and global networks, due to safety information in modern society, preparation of competent experts in cyber security in accordance with educational standards.

The basis for the professional development of the specialists of the industry is continuous education with the use of innovative pedagogy, the development and implementation of effective methods and methods of life-long learning, among which heuristic methods contribute to professional creative development. The organization of the training of future cyber security specialists should be considered in the concept of step-by-step continuing education and within the framework of social partnership between higher educational institutions, the state, business, domestic and international public organizations.

References

Bystrova B. V. (2017). Features of the formation of a system of professional training for future bachelors of cyber security in USA universities.Visnyk Cherkas'koho universytetu. Seriya «Pedahohichni nauky», vyp. # 6, 15–18. [in Ukrainian].

Bystrova B. V. (2017). Modernization of the educational program "Cyber Security": Realities and Prospects. Naukovyy visnyk Mukachivs'koho derzhavnoho universytetu, Seriya «Pedahohika ta psykholohiya». Vypusk 2 (6), 22–24. [in Ukrainian].

Dioritsa I. (2017). Educational standards for the training of cyber security specialists. Natsional'nyy yurydychnyy zhurnal: teoriya i praktyka, February, 2017, 50–53. [in Ukrainian].

Mel'nyk S. Conceptual foundations for the organization of professional training of future cybersecurity specialists. Pedahohichni nauky: teoriya, istoriya, innovatsiyni tekhnolohiyi, (2016). 2016, 10, 79–88. URL: http://nbuv.gov.ua/UJRN/pednauk_2016_10_9. [in Ukrainian].

Mel'nyk S., Voskoboynikov S. (2016). Features of the training of future specialists in the field of information security in cyberspace in the United States of America. Pedahohichna teoriya i praktyka, 2, 328–345. [in Ukrainian].

NICE official site. URL: http://csrc.nist.gov /nice/framework (30.11.2016).

American Military University official site. URL:: https:// www.amu. apus.edu (30.11.2016).

Information Assurance Workforce Improvement Program Department of Defense instruction DoD 8570.01-M URL: http://www.dtic.mil/whs/ directives/corres/pdf/857001m.pdf (30.11.2016).

Information Assurance and Security Education Center official site [Електронний ресурс]. – URL: https://iasec.eller.arizona.edu/programs/iace-courseware (30.11.2016).

International Association of Computer Investigative Specialists (IACIS) official site. URL: http://www.iacis.com (30.11.2016).

КІБЕРБЕЗПЕКА У СУЧАСНОМУ СОЦІУМІ ТА ВДОСКОНАЛЕННЯ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ГАЛУЗІ НА ЗАСАДАХ КОМПЕТЕНТНІСНОГО ПІДХОДУ

Сергій Воскобойніков, *кандидат педагогічних наук, старший викладач,*
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Сергій Мельник, кандидат технічних наук, доцент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Анотація. *В статті розкрито тенденції модернізації професійної підготовки майбутніх фахівців із кібербезпеки на засадах компетентнісного підходу: створення нових технологій відповідно світового рівня розвитку ІТ-технологій, нових сфер, спеціалізацій професійної діяльності та забезпечуються технологічним, управлінським рівнями професійної діяльності із забезпечення кібербезпеки у суспільстві, державі та для її громадян, міжнародного співробітництва і співпраці у галузі для ІТ-підтримки та безпеки електронного документообігу з використанням локальних і глобальних мереж, належного захисту інформації у сучасному соціумі, підготовку компетентних фахівців у галузі кібербезпеки відповідно до освітніх стандартів. Встановлено, що основоположною для професійного розвитку фахівців галузі є неперервна освіта із застосуванням інноваційної педагогіки, розробки й упровадження ефективних методів і методик навчання впродовж життя. Доведено, що організацію професійної підготовки майбутніх фахівців з кібербезпеки доцільно розглядати в концепції ступеневої неперервної освіти та в рамках соціального партнерства між вищими навчальними закладами, державою, бізнесом, вітчизняними та міжнародними громадськими організаціями.*

Ключові слова: *кібербезпека, інформаційне суспільство, ІТ-технології, вища професійна освіта, майбутня професійна діяльність, компетентний підхід.*

Література

Бистрова Б. В. (2017). Особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США. Вісник Черкаського університету. Серія «Педагогічні науки», вип. № 6, 15–18.

Бистрова Б. В. (2017). Модернізація освітньої програми «Кібербезпека»: реалії та перспективи Науковий вісник Мукачівського державного університету, Серія «Педагогіка та психологія». Випуск 2 (6), 22–24.

Діоріца І. (2017). Освітні стандарти підготовки фахівців із кібербезпеки. Національний юридичний журнал: теорія і практика, лютий 2017р., 50–53.

Мельник С. (2016). Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки Педагогічні науки: теорія, історія, інноваційні технології, № 10, 79–88. URL: http://nbuv.gov.ua/UJRN/pednauk_2016_10_9.

Мельник С., Воскобойніков С. (2016). Особливості професійної підготовки майбутніх фахівців із захисту інформації в кіберпросторі в Сполучених Штатах Америки // Педагогічна теорія і практика, 2, 328–345.

NICE official site [Електронний ресурс]. – Режим доступу : http://csrc.nist.gov/nice/framework (дата звернення: 30.11.2016).

American Military University official site [Електронний ресурс]. – Режим доступу: https://www.amu.apus.edu (дата звернення: 30.11.2016).

Information Assurance Workforce Improvement Program Department of Defense instruction DoD 8570.01-M [Електронний ресурс]. – Режим доступу : http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (дата звернення: 30.11.2016).

Information Assurance and Security Education Center official site [Електронний ресурс]. – Режим доступу: https://iasec.eller.arizona.edu/ programs/iace-courseware (дата звернення: 30.11.2016).

International Association of Computer Investigative Specialists (IACIS) official site [Електронний ресурс] – Режим доступу: http://www.iacis.com (дата звернення: 30.11.2016).