ENTREPRENEURSHIP MODEL OF CYBERNETIC SECURITY PROFESSIONALS

Oksana Portna, V. N. Karazin Kharkiv National University
Andriy Melikhov, Pryazovskyi State Technical University
Ievgeniia Dragomirova, Donetsk State University of Management
Irina Noha, Donetsk State University of Management
Ruslana Soichuk, Rivne State University of the Humanities

ABSTRACT

The formation of a system for the training of cyber security specialists was conducted in accordance with the national strategy and under the influence of economic and political factors in accordance with the social request and cyber security policy of the United States in order to protect civil rights and interests of the business, scientific, technical, military, financial potential and achievements of high technologies of the country, developing a responsible attitude towards national security in the US population. The basic principles of the organization of higher education of the USA are defined: decentralization of state-level education management; independence and complete autonomy of the higher educational establishment; equal functioning of state, private and semi-private higher educational establishments; possibility of free choice of students by disciplines; democracy, equality of opportunity for each person in obtaining higher education.

Keywords: Cybernetic Security, Information Society, Staff Assistance, Industry Standardization, Professional Competencies.

JEL Classifications: M5, Q2

INTRODUCTION

At the same time, the considerable opportunities and benefits of the proliferation of digital technologies have led to a number of social and ethical issues. There is growing public concern about the digital divide in different countries, the threat of online safety of citizens, and the health risks of using ICT. In addition, new types of crime occurred in cyberspace: abuse of information, violation of data transmission security, intellectual property infringement (plagiarism and piracy), online propaganda, radicalization. Separate crimes show violations of basic human rights: cyber-bullying, cyber-fraud, sex-traffic, pornography, identity theft, etc. Disturbing reports by heads of different countries on the negative impact of ICT force the national level to apply censorship or strict rules for its use and access to the Internet, filtering and blocking content. Security in cyberspace and the prevention of cybercrime are critically important factors in the welfare of society.

The urgency of the study is due to the rapid spread of information technology in all spheres of modern society, which requires high-quality training of professionals, who form a new generation of representatives of high-tech society, capable of transmitting, storing and processing information in cyberspace, resisting unauthorized interference in the information environment.

Citation Information: Portna, O., Melikhov. A., Dragomirova, I., Noha, I., & Soichuk, R. (2019). Entrepreneurship model of cybernetic security professionals. *Journal of Entrepreneurship Education, 22*(5).

With the development of the IT industry and the emergence of a new specialty Cyber Security specialty, the need to study the experience of foreign countries, the identification of constructive ideas about the training of IT professionals for their creative implementation in Ukraine is growing. The expediency of addressing the experience of the United States of America is confirmed by the need to establish new means of controlling the security of relations in the information space; the need to preserve the confidentiality of information, both public and private; US leadership in providing information services; creation of an effective system of preparation of specialists in cyber security, borrowed from many European countries; functioning of a powerful network of institutions of higher education, which trains competitive experts in cyber security on the world market.

REVIEW OF PREVIOUS STUDIES

An analysis of documentary and scientific sources indicates significant contributions from American researchers regarding the specifics of training IT industry professionals, in particular: studies that reveal the main points of cyber security and computer networks (Chapman, 2017); learning technologies, its impact on the effectiveness of the educational process (de Moura Gonzales & Portela, 2018); technologies of risk management of cyber threats (Drobyazko et al., 2019a); theory of a network society (M. Castells) (Hilorme et al., 2019a; Hilorme et al., 2019b); issues of global security, cyber defines and digital transformation, techno genic law, cyber confidentiality (Nagy & Lakatos, 2018), information technology and cyber security (Sarbu, 2017; Drobyazko et al., 2019b).

At the same time, the study of the source base suggests that the problem of the professional training of bachelors in cyber security in US higher educational establishments was not the subject of a separate study and requires a comprehensive scientific research.

METHODS

The methodological basis of the research is the leading position of the scientific theory of knowledge on the interaction and interdependence of the phenomena of objective reality; systematic, culturological approaches to comparative analysis of pedagogical phenomena; philosophical and pedagogical ideas about a proactive approach in the development of modern education; methodological principles of comparative-pedagogical research; ideas of comparative studies based on diachronic and synchronic study of pedagogical, socio-cultural and economic realities.

RESULTS AND DISCUSSION

Despite the fact that the national policy of any country involves the preservation and protection of borders and national sovereignty, infrastructure, equipment, and logistics of cyberspace operate outside of these borders, which gives it international status. The transnational nature of cyberspace requires solving problems through regional and international cooperation. In addition, in the measures to overcome the threats, the development of appropriate solutions to enhance the security of cyberspace at the national level, there is a need for cooperation in various sectors: political, economic, technological, legal, managerial, military.

In the modern information society, the dependence of the economic, political and social spheres on the information and cybernetic capabilities of the country is observed. According to expert estimates, the potential damage from cyber-attacks to online banking and financial services of only one European country will be over 10 million euros per day. Therefore, many countries have developed and approved a national strategy for cyber business, which was backed up by an appropriate legislative framework, and introduced national mechanisms for responding to cyber incidents. Some countries have proclaimed the cyberspace as the fifth military object, and also created protective and offensive cybercriminals in its armies in order to minimize the risks for industry and citizens.

However, the analysis of relevant materials shows the existence of different perspectives and approaches to solving the problem of cybernetic threats in different countries. There is a difference in the definition of responsible authorities: if in some countries national organizations responsible for managing cyber security have been established, then other responsibility for the implementation of national policy is assigned to the coordinating bodies, and policy management and implementation has been left to the government departments.

Despite the creation of national bodies responsible for the cyber security policy and the specifics of its implementation in each individual country, the international nature of cybernetic space requires the development and coordination of policies, primarily on the international level. Study of research materials suggests that the number of international organizations, governmental and non-governmental bodies responsible for global or regional cyber security is steadily increasing. Its activities range from research to regulatory, aimed at developing a collective approach to solving the problem of cyber threats.

An analysis of the legislative framework in the field of cyber security in different countries has made it clear that it is rather complex and varies very quickly, and the difference is observed in how countries interpret cyber security in national laws. Many countries and national organizations respect both national and international cyber security laws and report on certain types of financial or other types of cybercrime. There are international standards for law enforcement activities (cooperation implemented by Interpol). Many countries have adopted requirements for reporting on the commission of cybercrime. Today, work is under way to create an international code of cybernetics. The most influential international organizations implementing the policy of coordinating and regulating the activities of countries in the field of safe use of cyberspace include: UNESCO, NATO, U.S. Government Cyber Command, Europol, Cooperative Cyber Defence Centre of Excellence, CCD COE), European Agency for Networks and Information Security, ENISA), The International Organization for Standardization, ISO, Organization for Security and Co-operation in Europe, OSCE), Global Forum for Incident Response and Security Teams, the International Multilateral Partnership Against Cyber Threats, IMPACT, the Armed Forces Communications and Electronics Association, AFCEA, the Internet Corporation for Assigned Names and Numbers, ICANN, the Internet Governance Forum, IGF, the UN-backed International Telecommunications Union, ITU.

The most common and most popular types of certification for the *“Cyber Security Specialist”* in the world are: CEH: Certified Ethical Hacker; CISSP: Certified Information System Security Professional; CCSP: Cisco Certified Security Professional, and for the *“Information Security Specialist”*: CISA: Certified Information Systems Auditor; ISO 27001-Lead Implementer; SO 27001-Lead Auditor.

The result of the implementation of the US cyber security policy and its impact on the process of providing the industry with cyber security personnel was the introduction of a number of measures to address the shortage of personnel that is schematically presented in Figure 1.

As a result of the intensive expansion of the cyberspace of American society and the growing role and strategic importance of cyber security, human resources provision of the IT industry provides for the following areas: recognition of the training of cyber security specialists as an important stage in the implementation of the national strategy in the context of cyber security policy; standardization of training of specialists in the IT industry; development of programs for training specialists, as close as possible to the practical needs of the industry and international certification requirements; introduction of the latest pedagogical technologies in the process of training specialists, such as: dual, blended learning, practice-oriented learning; popularization of specialties and motivation of talented youth with the purpose of greater interest in obtaining a specialty and increasing the prestige and popularity of professions related to cyber security; a steady increase in investment for the IT industry for its further development with a tendency for job growth for cyber security professionals; growth in the need for highly skilled management personnel; increasing the role of higher education to prepare a highly skilled cyber security elite.

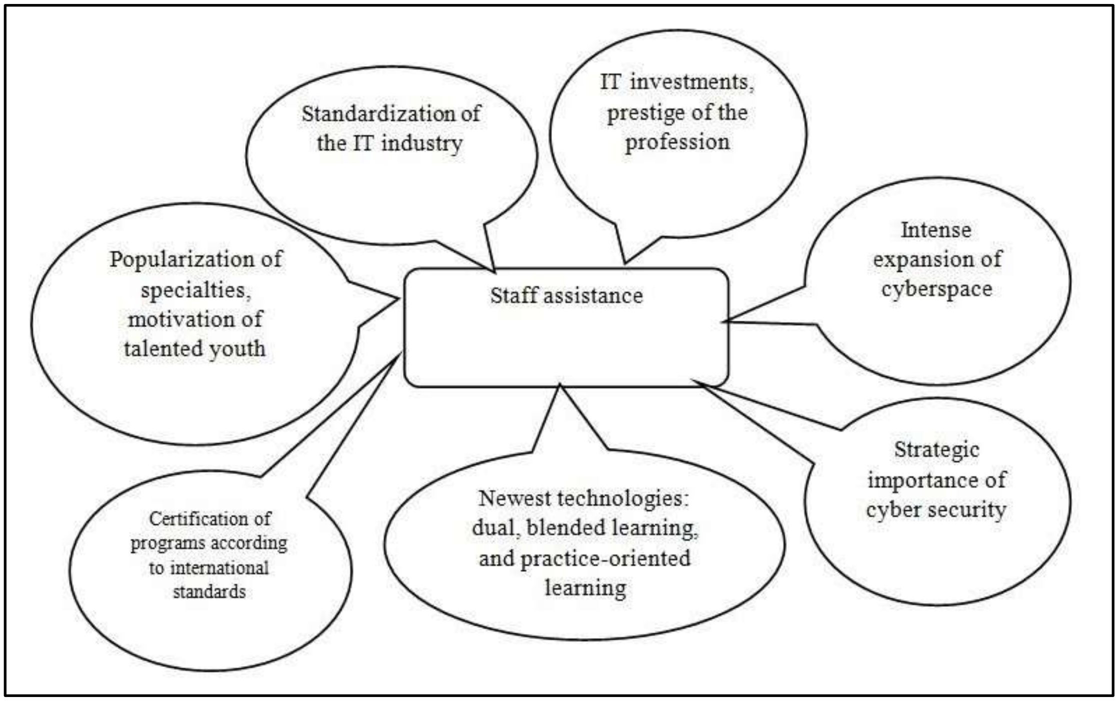
Standardization of the IT industry
IT investments, prestige of the profession
Popularization of specialties, motivation of talented youth
Staff assistance
Intense expansion of cyberspace
Strategic importance of cyber security
Certification of programs according to international standards
Newest technologies: dual, blended learning, and practice-oriented learning

FIGURE 1
LEADING TRENDS IN STAFF ASSISTANCE OF THE IT INDUSTRY, CYBER SECURITY SPECIALTY (AUTHOR'S DEVELOPMENT)

The results of our study are confirmed by the following studies. At the current stage, the training of cyber security personnel is not only a response to market demand in such specialists, but also serves as an important component of the state measures to counter threats in cyberspace (Sarbu, 2017). Accordingly, the structuring of the contents of the training of these specialists takes place and clear requirements are set for educational institutions in the organization of such training. In the general system of providing cyber security of the state, staff assistance is an independent subsystem, and the system of training specialists is the basis of such support.

RECOMMENDATIONS

The international nature of the cybernetic space requires the development and coordination of a common policy for all countries of the world regarding guarantees of safe use of cyberspace. On the basis of the analysis of international normative and legal documents, the main directions of activity of international organizations in the field of cyber security are recommended: creation of legal basis for international cooperation of different countries, unification of efforts to prevent and timely response to cybercrime, effective training of personnel capable of guaranteeing safe use of information and communication networks.

CONCLUSION

At the present stage of science and technology development, the cyber security of the country is becoming one of the most important branches of high-tech society. Due to the widespread use of modern information technologies in all spheres of existence, the society has become vulnerable to cybernetic influences, which increasingly become an effective tool for achieving non-bearing control and management of both infrastructure objects of the state, enterprises, as well as individual citizens and their associations. The streams of information being transmitted, stored and processed in cyberspace are constantly increasing, requiring its proper protection against unauthorized access with a criminal purpose.

It is obvious and indisputable that in the conditions of further development of high-tech society the need for specialists in cyber security will be constantly growing.

It was found out that the methodological basis for studying the problem of professional training of cyber security specialists was the following approach: competence-based, within which professional training is considered as a process of assimilation and consolidation of general and special knowledge and skills for effective performance of professional tasks of the future workplace of IT-industry; functional, which establishes the dependence of the process of professionalization of future cyber security specialists on the peculiarities of the activity of educational institutions; instrumental, emphasizing the importance of mastering the system of skills through the application of appropriate methods and forms of organization of educational process; person-oriented, defining a future cyber security specialist as a highly professional person; axiological, studying professional training of cyber security specialists as a process of formation of their professional qualities taking into account the values of society.

The study does not cover all aspects of this urgent problem. To further directions of scientific research, we consider it expedient to include: didactic substantiation of the peculiarities of the professional development of IT staff in the USA; psychological, pedagogical and organizational principles of IT specialists training for pedagogical activity in the conditions of integration of the educational and industrial sectors.

REFERENCES

Chapman, R.E. (2017). *Public-private partnerships pay big dividends: A case study of cybernetic building systems.* Hvac & R Research.

de Moura Gonzales, S.L., & Portela, L.S. (2018). The geopolitics of the South American cybernetic space: The (non) shaping of security policies and cybernetic defense? *Brazilian Journal of Strategy & International Relations, 7*(14), 209.

Drobyazko, S., Hryhoruk, I., Pavlova, H., Volchanska, L., & Sergiychuk, S. (2019a). Entrepreneurship innovation model for telecommunications enterprises. *Journal of Entrepreneurship Education,* 22(2).

Citation Information: Portna, O., Melikhov. A., Dragomirova, I., Noha, I., & Soichuk, R. (2019). Entrepreneurship model of cybernetic security professionals. *Journal of Entrepreneurship Education, 22*(5).

Drobyazko, S., Potyshniak, O., Radionova, N., Paranytsia, S., & Nehoda, Y. (2019b). Security of organizational changes via operational integration: ensuring methodology. *Journal of Security and Sustainability Issues 9*(1), 1595-1612.

Hilorme, T., Shurpenkova, R., Kundrya-Vysotska, O., Sarakhman, O., & Lyzunova, O. (2019a). Model of energy saving forecasting in entrepreneurship. *Journal of Entrepreneurship Education, 22*(1S).

Hilorme, T., Zamazii, O., Judina, O., Korolenko, R. & Melnikova, Y. (2019b). Formation of risk mitigating strategies for the implementation of projects of energy saving technologies. *Academy of Strategic Management Journal*, *18*(3).

Nagy, E., & Lakatos, A. (2018). Threats in the security policy of the USA. *GeoJournal of Tourism & Geosites, 20*(1).

Sarbu, S. (2017). The cyber threat and the problem of information security. A critical analysis of the concepts of cyber-power and cyber-space. *Annals–Series on Military Sciences, 9*(1), 126-138.

Citation Information: Portna, O., Melikhov. A., Dragomirova, I., Noha, I., & Soichuk, R. (2019). Entrepreneurship model of cybernetic security professionals. *Journal of Entrepreneurship Education, 22*(5).