DOI: 10.1515/rpp-2017-0058

Senior Lecturer, **BOGDANA BYSTROVA**
National Aviation University
Address: 1 Kosmonavt Komarov St., 03058, Kyiv, Ukraine
E-mail: danabystrova@gmail.com

COMPARATIVE ANALYSIS OF CURRICULA FOR BACHELOR'S DEGREE IN CYBER SECURITY IN THE USA AND UKRAINE

ABSTRACT

At the present stage of science and technology development the need to strengthen cyber security in every developed country and transform it into one of the most important sectors of society is growing. The peculiarities of the professional training of cyber security bachelors in the U.S. higher education system have been defined. The relevance of this approach is determined by the dynamics of technological advances. An innovative approach is a methodological platform for research and students' project work, their communication with professional scientific community on the stage of the national strategy on cyber security implementation. The results of the comparative analysis of educational programs for cyber security bachelor's degree in the U.S and Ukraine have been presented. At the stage of the national strategy on cyber security implementation there has been made an emphasis on a specific task – to provide a balance between the objectives and results of education for the inner harmony of study process. We have indicated a number of key tasks, as follows: standardization, implementation of dual and mixed types of training, the promotion of new technologies in the educational process; provision of the motivation of students. The conducted research of American experience concerning professional training of cyber security bachelors will enable to determine the possibilities of its progressive ideas implementation into higher education of Ukraine (in particular, the improvement of industry standards for cyber security bachelor's degree; providing the information support of Internet resources; development and improvement of the content of curriculum and educational programs for training bachelors of cyber security; improvement of educational and methodical implementation; advanced study of foreign experience. The successful implementation of reasonable opportunities will promote professional training of national experts in the field of cyber security, accelerate the process of reforming the national higher education system, convergence of the international educational standards, and ensure its competitiveness in today's job market.

Keywords: *higher education, the USA, cyber security*, development, *bachelor, standardization, dual training, mixed training.*

INTRODUCTION

Nowadays, under the conditions of science and technology development in USA, the need to strengthen cyber security and transform it into one of the most important sectors of society is growing. Through attacks on critical infrastructure, the development of the Internet, the 4th industrial revolution, cyber attacks, and the rise of global instability, there is a need for the development of the cyber security industry. Due to the extremely wide use of modern information technologies in all spheres of its existence, the society has become vulnerable to cyber influences, so there is a need for non-control and management of objects of critical infrastructure and separately enclosed citizens or their associations. An information flow which is transmitted, stored and processed in cyberspace is also constantly growing; in this way there is a need for its proper protection against unauthorized access. There is an urgent need for specialists in cyber security and it will continue to grow with the further development of high-tech society.

The quality of specialists' training in the field of cyber security is determined by the level of technological development of the country, but to answer the question of how this training meets modern requirements, there is a need for a comparative analysis of the cyber security specialists' training in other countries. We compared some similar cyber security bachelor educational programs on the subject of organization, technology, content and learning outcomes in universities of Ukraine and the United States.

THE AIM OF THE STUDY

The purpose of the paper is to present the results of the comparative analysis of educational process on cyber security curriculum in universities of Ukraine and the United States**;** to highlight the results of cyber security national strategy implementation in Ukraine, taking into account main obstacles, ways of overcoming them and the main tasks of the educational system for the mentioned industry; to analyze the strategy of educational program modernization in the field of cyber security in universities of Ukraine with an emphasis on the special task of ensuring the balance between the objectives and results of the education, the inner harmony of the subjects of study.

THEORETICAL FRAMEWORK AND RESEARCH METHODS

The curricula for Bachelor's degree in cyber security in the USA and Ukraine have been studied based on the works by Ukrainian and foreign scholars (E. Chabrow (2015), I. Diorditsa (2017), D. Dubov (2010), V. Kovalenko (2010), J. Franscella (2013), M. Moore (2005), C. Watson (2005), L. Zubyk (2016)) as well as some normative documents (The National Security Strategy of the United States of America, The Strategy Project of Providing Cybernetic Security of Ukraine).

This work has been performed under the critical-dialectical approach, using research methods of analysis, synthesis, comparison and generalization that are necessary to study the original texts and official documents, organization of the studied material and its exposure.

RESULTS

A detailed comparison of the educational programs of the United States and Ukraine universities according to the content and the learning outcomes enables to evaluate each program as a whole and the level of teaching the main disciplines. The analysis has been specified by comparing the North American Carolina Cyber Security Bachelor Degree Program (NCSU) and the Cyber security Program of the Higher Education Institutions of Ukraine. In Ukraine, the specialists' training in higher educational establishments is regulated by the state educational standards and every five years it is subjected to consideration by the Accreditation Commission of Ukraine (ACU). There are no state educational standards in the United States, but each university accredits its educational program in specialized agencies that set the same requirements for each program, and every six years confirms accreditation. The Accreditation Council for Engineering Sciences and Technology (ABET, www.abet.org) serves as the agency's Cyber Security program. The scope of accreditation (3000 programs) allows us to talk about their unification. In Ukraine, since 2013, cyber attacks have gained a new status ("cyber war"), the annual growth in the rate of cyber attacks is 40 %. Ukraine does not have sufficient resources to ensure a worthy confrontation. The number of certified cyber security specialists in the world is 108 thousand people, among them the absolute leader is the United States – 71 thousand people, while in Ukraine –

18 people, and it's the 78th place in the world. Studying the scientific achievements and best practices for training bachelors in cyber security in the United States allows us to define the tasks and ways of further modernization of the specialists' training system in this industry in Ukraine.

For a comparative analysis of the organization and educational technology processes in the United States Universities, the NCSU (North Carolina State University) and its engineering faculty (Cyber Security) have been selected. NCSU consistently holds high places in the US News and World Report (2015 – the 31st out of 150). In Ukraine, 30 universities train specialists in the field of "cyber security". Every year, 800 bachelors graduate, while the need is 2000 per year (based on calculations on the number of cyber attacks). The NCSU trains IT professionals in one program, with 50 lecturers from the same department, with 1300 graduates and postgraduates each year. The Cyber Security curriculum in the NCSU and in Ukraine has a similar structure and focus. Among the features of NCSU is that high school students can be enrolled in separate university courses, passing exams with students, and then, after the entry, the previously obtained results are counted. A college graduate who enters the NCSU, on the received results, also has a transfer credit. Research findings by E. Chabrow (2015) proves that in universities of Ukraine only graduates of specialized colleges and universities can undergo a short-term training program (2.5 – 3 years) to obtain a bachelor's degree. In US schools, IT in most states (North Carolina included) is not a compulsory subject. Therefore, computer science is taught during two first years of studying. In Ukraine, computer science is a compulsory subject at school, and after taking the cyber security major, there is a need for the External Independent Evaluation (EIE) in IT and computer science which is a compulsory course in further education (Franscella, 2013). Many researchers at NCSU consider that a student who graduates with a bachelor's degree in cyber security enters an engineering faculty and is obliged to study a minimum of disciplines (English, Mathematics, Chemistry, Physics, Entry into Engineering) and choose the main program, while additionally choosing a shortened version of another program (Moore, 2005). In our universities the student immediately enters a particular field of study, and mastering another educational program is theoretically possible, but is usually an exception. During 4 years of studying at the NCSU, a student must study a minimum of 40 disciplines to get a bachelor's degree (45 – in 2015–2016). Among them there were 23 majors and 17 electives. In Ukraine, according to a similar program, student studies 45 disciplines. The ratio of general subjects to core ones is 1:1. Students can also choose to take elective subjects which make up 20 %. The analysis showed that curriculum and course requirements in Ukraine are incomplete with core disciplines, there is insufficient number of hours and the lack of disciplines standardization. The courses and topics formation is not related to the need of the market and university entrants, but to the availability of departments and teachers and in respect to the elective disciplines According to the National Security Strategy of the United States of America (2013), to study at cyber security course in NCSU it is necessary to get at least 120 credits (1 credit is 15 lecture hours, the lecture lasts 75 minutes).

In Ukrainian Higher Educational Institutions (HEIs) for the majority of courses 1 credit hour equals 30 academic hours and lecture duration is 90 minutes. Lists of disciplines are very similar. At the same time, the number of classroom hours varies from 2000 in NCSU to 2840 in HEIs, due to the almost total absence of practical and laboratory classes on special training disciplines in the NCSU. The ratio of hours between lectures and practical classes of the studied programs varies greatly. The NCSU is dominated by lecture classes, and in many disciplines there is no practical work. In Ukraine, the ratio between lectures and practical classes is about 1:2.

Ukrainian students perform a significant part of the tasks in the classroom with the help of a teacher; NCSU students perform tasks independently as homework. NCSU students practically do not write lectures, because the lecturer puts a large amount of information online and encourages students to use a particular textbook, which is going to be followed in the lectures. Ukrainian students mostly take notes of a lecture because the teacher does not associate one course with one textbook and there is a lack of educational material on the site. NCSU does not have oral exams of reporting, similar to the Ukrainian "credited" ones. In the NCSU, an examination and assessment system is announced for each discipline at the beginning of the semester. At universities in Ukraine, an exam does not play a decisive role in the assessment, which is the ratio of the results of practical classes and the exam for the semester. In the NCSU, an exam cannot be "retaken", but it is possible to repeat the course. In Ukraine, re-examinations are still practiced.

The final exam exists for each discipline and includes tasks of three types: with a selective answer, an answer in the form of a number or a short line and a detailed answer. The exam duration is 3 hours. In Ukraine, most of the exams are taken orally, containing questions from the list (known to students). Students at NCSU often receive test samples from different levels of difficulty from the examiner. In the NCSU, an assessment system for the exam is announced for each discipline at the beginning of the semester. In the universities of Ukraine, exams do not play a decisive role in the formation of the assessment, which is the ratio of the results of practical classes and the exam for the semester. Studying at NCSU is fee for all students (some can get support from different funds). In 2015–2016 full tuition fees for the bachelor's degree in Cyber Security for residents of North Carolina amounted to about $20,000. In Ukraine, the ratio of state-sponsored vacancies for full-time attendance study is 1:1.

The study programs of both countries take into account the regulatory requirements for the training results – the State Educational Standard (SES) in Ukraine and the Applied and Natural Science Accreditation Commission (ANSAC) for NCSU. In both cases, the requirements relate both to the learning outcomes and to the conditions for its implementation, and on these requirements the advanced educational programs are developed. According to researchers in the United States, "traditional certification" is a training program based on 4-year colleges in the field of "education", which involves the students' preparation and their acquisition of competence, which is assessed through the examination in accordance with state requirements (Kovalenko, 2010). According to D. Dubov, Ukraine has real problems with the educational training of cyber security specialists because of unavailability of graduates to take international professional examinations and work on a specialty; lack of practical skills for graduates (Dubov, 2010). The overall structure of training in NCSU and Ukraine is similar – in both cases the percentage of humanitarian, mathematical, natural sciences and specialist disciplines is approximately the same.

According to DHS, training in the US involves a number of skills which a specialist must obtain on completion of university training, namely: to understand important terminology, materials, technology; be able to possess general skills in cyber security; have a fairly high level of skills to understand the system, monitor security systems, using network screens and intrusion detection systems; be able to create, implement and monitor the implementation of security policy, act according to the emergency data recovery plan for operating systems, databases, networks, servers and applications; conduct research of new products, services, protocols and standards for increasing the safety level; carry out regular checks on the suitability of use (Watson &Cynthia, 2008). The main tasks of improving the training system for cyber security specialists at the stage of national strategy on cyber security implementation are as follows: to standardize the requirements for training specialists; develop a training curriculum in accordance with the practical needs of the industry and the international certification requirements; encourage the latest learning technologies; introduce dual and mixed types of studying; popularize the specialty by encouraging specialists; provide motivation for the teaching staff (DHS, 2012). Research findings by L. Zubyk give results of the analysis of bachelors' training in information technology structure that help to make conclusions about cyber security structure of bachelors' training (Zubyk, 2016).

Research findings by I. Diorditsa and L. Zubyk prove that in order to implement the cyber security Strategy of Ukraine for 2017–2018, a number of promising steps are planned: a) approval of the educational standard for the specialty; b) development of educational materials for the first two years on the platform of distance education; c) launching the educational program from September 2017; d) formation of the dual education platform, involving leading Ukrainian and international companies; e) development of educational materials for professional disciplines for the third and fourth years of study; f) development of on-line cyber security training platform for mixed studying; g) creation of a community of lecturers and experts on cyber security (Diorditsa, 2017) .

According to the National Security Strategy of the United States of America and Higher Education in the US the modernization of higher education system for training undergraduates in cyber security provides the following results: a) after the 2nd year of study English level should be B2; b) the development of "Soft Skills" that can be successful regardless of the activity specifics (skills to persuade, have a way with people, work in a team; which have the characteristics of erudition, creative thinking, leadership, negotiation skills, professional language skills, work with information); c) all preparatory disciplines are subordinated to professional ones and taught at the first and second years; d) during the 3rd and 4th years the vocational training is carried out through dual education and free access to the online platform of the mixed type of training; e) the training program is subjected to the requirements of the international certification programs CISSP, ISACA and standard job descriptions of the leading companies in the world (The National Security Strategy of the United States of America, 2015; Higher Education in the US, 2016).

CONCLUSIONS

Today, according to the state program of educational standard modernization of the cyber security course, the recommendations to the structure and content of the methodical guidelines have been developed; also, the structure of preparatory disciplines has been formed; the work on preparation of academic curricula for the first and second years of study (2017–2019) and preparation of educational materials for preparatory disciplines has been started; a round table with participation of the Ministry of Education and leading universities of the country has been organized. It is planned to make free access to online platform of the mixed type of training, create a community of lecturers and experts in cyber security. Five universities have already been involved in the project, which is a critically small number at the moment. The emphasis is placed on increasing the credibility of the universities in Ukraine by employers and entrants.

Further research should study and analyze the peculiarities of dual education (50% of studies and 50 % of internships) at universities and the competitiveness of Ukraine in the global market of cyber security.

REFERENCES

1. Chabrow, E. (2015). *Cyber security as a Campaign Issue.* Retrieved from http://www.govinfosecurity.

2. DHS. (2012). Task Force on Cyber Skills. *Cyber Skills Task Force Report. D.o.H. Security.* Washington, DC, 1–41.

3. Diorditsa, I. (2017). Kvalifikatsiyni vymogy do kompetentsiy fakhivtsiv z kiberbezpeky. *Informatsiyne pravo*, 2, 215–219.

4. Dubov, D. (2010). Kiberbezpekova polityka u konteksti transformatsii polityky bezpekt USA administratsyi B. Obamy. *Politychnyi Management,* 1, 155–163.

5. Franscella, J. (2013). *Cybersecurity vs. Cyber Security: When, Why and How to Use the Term.* Retrieved from http://www.infosecisland.com/blogview/23287-

6. Higher Education in the US. (2016). *Higher Education in the US.* Retrieved from http:// www.iclass.ru/study_abroad_high_usa/.

Kovalenko, O. (2010). Neperervna pedagogichna osvita USA: suchasnyi stan perspectyvy rozvytku. *Teaching science: theory, history, innovative technology,* 6 (8), 127–132.

7. Moore, M. (2005). *Distance Education: A System View.* Belmont CA: Wadsworth Publishers.

8. The National Security Strategy of the United States of America. (2015). *The National Security Strategy of the United States of America.* Retrieved from https://www.state.gov/documents/organization/63562.pdf.

9. The Strategy Project of Providing Cybernetic Security of Ukraine. (2013). *The Strategy Project of Providing Cybernetic Security of Ukraine.* Retrieved from http://www.niss.gov.ua/public/File/.

10. Watson, C. (2008). *U.S. national security: a reference handbook*. Santa Barbara, California: ABC-CLIO.

11. Zubyk, L. (2016). The Analysis of Structure of Training of Bachelors in Information Technology. *Molod and Rynok,* 3 (134), 173–174.