UDK 004.056.5 *DOI 10.36074/pmepocs.ed-1.01*

Igor Diorditsa[1]

EDUCATIONAL STANDARDS FOR TRAINING OF CYBER SECURITY PROFESSIONALS: LEGAL AND ORGANIZATIONAL ISSUES

ABSTRACT:

The article explores the problems of legal and organizational principles of formation of cybersecurity specialists and the issues of improvement of normative regulation of the processes of training of professionals in the specified field. It is established that the interest of scientists to educational standards has recently increased significantly due to the revision of the essence of the concept in the Law of Ukraine «On Higher Education» of 01.07.2014, the closer link between standards and quality of education. At the same time, active attention is paid to the issues of constituent standards of higher education, implementation of the competence approach and its reflection in the educational standards of the next generation. The theory and the newest practice of creating educational standards for the preparation of higher education students in the specialty «Cybersecurity» on the principles of integration of legal and pedagogical science are analyzed. The basis of the legal regulation of higher education standards in accordance with the new legislation has been established. The main components of educational standards in the content of education in the specialty «Cybersecurity» are represented and the legal component is highlighted in educational standards. Actual problems of standardization of education in training of cybersecurity experts are revealed. The scientific substantiation of the qualification requirements for cybersecurity specialists on the basis of the competence approach is offered. The essence of the concept of «qualification requirements», its components and the degree of representation of the key concept in terms of competencies of cybersecurity experts are determined. Qualimetric indicators of activity of this category of specialists are detailed. Improvement of educational standards of cybersecurity specialists is proposed by specialization of such specialists for further activity, first, in the following spheres: sphere of state power and management - introduction and support of processes of secure e-government, state information resources, ensuring unobstructed work of information analytics, statistical analysis, statistical analysis counteracting cyber attacks on websites of government agencies and organizations, etc; security and defense - activities in the context of ensuring national and information security in cyberspace; combating cybercrime, including cyber-terrorism, combating cyber-threats to military character, protecting the interests of the state by computer and technology warfare in information and hybrid wars; ensuring the operational state of cryptographic information security; economic sphere - prevention of cases of

[1] D.Sc. (Law), Associate Professor, Professor of the Department of Private and Public Law
Kyiv National University of Technologies and Design, UKRAINE

industrial espionage, theft of know-how, computer fraud with electronic payment documents, seizure of confidential economic data, illegal activities with payment and credit cards; theft of funds from electronic accounts, ordering goods and services at someone else's account, etc.; science and technology - counteracting cyber-espionage, developing software that prevents intrusion into computer systems, spreading viruses, destroying databases and more.

INTRODUCTION.

The complex tasks facing the state in the way of protecting its institutions, society, citizens from criminal encroachments on their rights, freedom in the information and communication space, require a comprehensive approach to work with professionals who are called upon in their professional activity to ensure cyber security. This approach should have a comprehensive scientific justification.

Formation of specialists is one of the main tasks for the labor market replenishment by qualified professionals, able to perform at the present level their functions. Therefore, this aspect cannot be ignored by scientists. For the most part, this problem is highlighted in scientific works on pedagogy, in particular, the formation of subjectivity (S. Pylypchuk), professional abilities (A. Klochko), professional skills (V. Yelov, V. Monastyrsky), professionally significant qualities (V. Savishchenko). professional culture (I. Mikhailichenko, M. Podberezsky, V. Rayko) of future specialists. Psychological foundations of forming a specialist as a subject of legal activity were investigated by N. Evdokimova. There are a number of publications on cyber security training in the area of knowledge «Information Technology» (V. Buryachok, Y. Danik, S. Demedyuk, V. Markov, A. Minockin, Y. Suprunov, etc.).

At the same time, the question of the legal and organizational foundations of cybersecurity training has not been a separate subject of scientific research. Solving this problem will subsequently improve the regulatory framework for the training of professionals in the field.

EDUCATIONAL STANDARDS FOR CYBERSECURITY TRAINING.

The intensification and intensification of the fight against cybercrime has raised questions for the world community about the need to train a fundamentally new category of professionals to protect the computer environment from criminal attacks on economic and political freedoms, state secrets, and more. In the context of Ukrainian reality, the problem is

complicated by information wars, attacks on the integrity and sovereignty of the state. In this regard, the training of cybersecurity professionals ceases to be pedagogical and should be systematically investigated.

Scientists' interest in educational standards has recently increased significantly due to the revision of the essence of the concept in the Law of Ukraine «On Higher Education» of 01.07.2014 [1], the implementation of a closer link between standards and quality of education. On the pedagogical basis the issues of standardization of higher education have been fruitfully developed by S. Gordiychuk [2], N. Zhuravskaya [3], O. Kiselyova [4], S. Strelets [5], S. Terepyshchim [6] and others. At the same time, active attention is paid to the issues of constituent standards of higher education, implementation of the competence approach and its reflection in the educational standards of the next generation.

According to the Resolution of the Cabinet of Ministers of Ukraine of April 29, 2015 No. 266 [7], a new specialty Cyber Security provides the need for theoretical understanding of the educational standards of training of specialists of the specified direction on legal grounds, which has not been practiced so far.

The purpose of this section is to analyze the theory and current practice of creating educational standards for the preparation of higher education students in the specialty «Cybersecurity» on the basis of integration of legal and pedagogical science. Achieving this goal is possible provided that the following tasks are solved: 1) establishing the basis for regulatory regulation of higher education standards in accordance with the new legislation; 2) representation of the main components of educational standards in the content of education in the specialty «Cybersecurity»; 3) highlighting the legal component in educational standards; 4) Identification of actual problems of standardization of education in training of cybersecurity specialists.

The task of designing educational standards for cybersecurity training for compilers is fundamentally new for two reasons: 1) the specialty was introduced for the first time, and therefore, only foreign experience in training similar specialists can serve as a sample; 2) The Law of Ukraine «On Higher Education» of 01.07.2014 made fundamental changes to the understanding of standardization of education and the processes that accompany it. Article 10 of the said Law interprets the standard of higher education as «the set of requirements for the content and results of educational activities of higher

education institutions and scientific institutions at each level of higher education within each specialty» [1]. It should be noted that the definition is not about the content of education, that is, an idea of what to teach, what subjects and topics to include in curricula and programs, but the essence of the activity of a higher education institution. We compare with the definition of the same term contained in the previous Law, where the standard of higher education was proposed to be understood as «the set of norms that determine the content of higher education, the content of training, the diagnostic tool for higher education quality and the normative term of education» [8]. So, in our opinion, the interpretation of the educational standards in the wording of the Law of Ukraine «On Higher Education», which became invalid, more favored the targeted training of specialists, specified instructions for answering the question: what and how to learn, what time of study and at what time a way to check the quality of training of a future professional.

In the previous law, along with the concept of «higher education standard» used the concept of «professional standard» - «approved in accordance with the established requirements for knowledge, skills and graduates of higher education institutions, which are determined by employers and serve as a basis for the formation of qualifications", which in the new The law is not explained, but only used with the phrase "when available» [8].

Therefore, the transformation of requirements by educational standards has taken place on the basis of a methodology based on the principles of autonomy of higher education institutions. Unlike the standards of the previous generation, which provided for a certain set of regulatory disciplines with quantitative indicators of hours allocated to their teaching, the standards of the new generation are oriented towards learning outcomes, and the content of education should be shaped by the higher education institution itself. This model follows Western approaches, where the university is responsible for the quality of its graduate training, for its competitiveness in the labor market.

Thus, according to paragraph 3 of Article 10 of the Law of Ukraine «On Higher Education» of 01.07.2014, the requirements for the educational program are standardized, which provides: the volume of credits of the European credit transfer system for each degree of higher education, the list of competences of the graduate, the normative content of the preparation of the higher education applicant, which is formulated not through the description of the disciplines, but through the results of training; forms of certification;

requirements for the system of internal quality assurance of education, as well as if there are requirements of professional standards [1].

At the same time, the drafters of the Law on Higher Education were not able to give 100% to all higher education institutions in the standards of higher education, as is the case in Western universities. Paragraph 6 of Article 10 of the said Law leaves the central executive authority in the field of education and science the right to set higher education standards for each specialty, taking into account the proposals of sectoral state bodies to the sphere of management of which belong to universities, as well as industry associations of employers' organizations. The approval of higher education standards is carried out according to the established norms in agreement with the National Agency for Quality Assurance in Higher Education.

The importance of developing standards for this specialty is evidenced by the fact that on October 3, 2016, at the Ministry of Education and Science of Ukraine, with the participation of Minister L. Grinevich, a round table was held dedicated to the training of cybersecurity experts [9]. The Minister emphasized the demonstration of new approaches to higher education standards created through interaction with employers and those who place orders for certain professional qualifications. The opinion of the director of the investment company Rayter INC (USA) Gregory Rayter was also right that, in creating standards for training bachelors in Cybersecurity, it is necessary to focus on the certification programs of professional associations, on the basis of which job descriptions are made. Thus, one can get as close as possible to the needs of practice and make the educational process as efficient as possible [10]. However, the existence of such certification programs is a reality of life for American and not Ukrainian society. Therefore, the standardization processes for the education of cybersecurity professionals provide an opportunity not only to cover the activities of higher education institutions, but also to raise issues before employers' associations regarding the development of certification programs similar to other countries.

Also, according to the American specialist, in educational programs should be given priority to practically oriented disciplines and foreign language, and only then - to the general disciplines. Such a pragmatic approach is inherent in American higher education, but is fundamentally new to Ukrainian higher education, which has traditionally been dominated by fundamental training. So, it is time to address another issue in standardizing education for the

Cybersecurity specialty: what proportion of the theoretical and practical components of the learning process should be represented, and whether the preparation of higher education students in the field of Information Technology will have a reserve of time to acquire legal competencies mastering the legal framework of information law, intellectual property law, regulatory support for cyber activity.

The event indicated that the leadership of the Ministry of Education and Science is aware of the importance of training cybersecurity professionals, but at present there are no educational standards for the specified specialty at the state level.

Since the preparation of higher education standards for cybersecurity majors is a fundamentally new phenomenon, there are many questions about the different aspects of designing standards, especially the content of education itself, including the essence of specialization.

It seems to us that the main problem in standardizing cyber security training is that nowadays this type of professional activity is outside the clearly defined legal field. Such activity is not envisaged by either state standards, in particular the Classifier of Economic Activities, the Classifier of Occupations, or clearly defined qualification characteristics, approved in accordance with the established procedure at the state level. Therefore, when conducting career guidance among high school graduates, college graduates interpret in their own way approximate lists of positions that may be further occupied by graduates. So, on the Sumy State University website it is stated that upon graduation in Cyber Security specialty, graduates with bachelor's degree can be software development and testing specialists, information technology specialists, computer program specialists, system administration technicians, etc. [11]. Familiarity with the above list of questions raises the question: where is the specificity of cybersecurity? Can higher education students who have studied in other specialties in the field of information technology know? Do education programmers generally understand what falls within the remit of a cyber security professional? Due to lack of coordination of higher education institutions with employers, close cooperation between universities, which are responsible for the training of such specialists, lack of systematic attention to science-based design of this specialty by the Ministry of Education and Science lead to the fact that licenses for educational activities taking into account a clear vision of the state-level tasks facing cybersecurity professionals.

It turns out that specialists are already preparing, but educational programs concluded by universities do not adjust with the list of competencies that should be approved at the state level. Practically, a situation arises when the archives of the public sector are paid for higher education, each of which in its own way interprets the idea of a dynamic combination of knowledge, skills and competencies that a higher education major in Cybersecurity should have.

The analysis of the curricula of some higher education institutions, in particular the National Technical University of Ukraine «Kyiv Polytechnic Institute», provides an opportunity to establish that the training of bachelor's and master's degrees in the specialty «Cybersecurity» is conducted in two specializations: «Systems and technologies of cybersecurity methods and" cybersecurity». In other universities specializations within the specified specialty are not distinguished.

According to existing approaches, bachelor's training involves 240 ECTS credits (7200 hours), and a master's degree – 120 credits (3600 hours). Considering that, according to the Law on Higher Education, approved by the Law of Ukraine, 60 credits (1800 hours) should be allocated for one academic year, this means that Ukraine will receive the first full master's degree in Cyber Security in six years. By this time, the state should be «comforted» by specialists who have been retrained after obtaining higher education in other specialties. This situation shows that, in the absence of strategic planning in the field of education, we are already falling short of the needs of the state and society, and of the challenges posed by the cybercrime world.

Accordingly, we would like to enter into a discussion with the drafters of the analytical report «The Training System for the Ukrainian Security Forces: Problems and Prospects for Development» prepared under the auspices of the National Institute for Strategic Studies [12]. It is not clear why, in the presence of the Law of Ukraine on Higher Education, the definition of «European Credit Transfer Cumulative System» and the indication that one ECTS credit is 30 hours, the drafters of the report choose the other path and indicate that one credit equals up to 8 hours of teaching activity [12]. As a result of an incorrectly chosen system of calculations, including in it as obligatory for all applicants of higher education of degrees of the bachelor and the doctor of philosophy, they come to the fact that the specialist receives preparation for 12 years [12]. Such an «error» can be costly for the society, since it misleads the government, specialists in the formation of the state budget, in particular in terms of

calculating the costs of training higher education applicants, as well as customers of future professionals. Due to such incompetence, there is a misunderstanding of deviation from the statutory educational standards of standardization, and disorganization is introduced into the activities of the relevant bodies. This is unacceptable.

In our view, modeling of educational standards in the specialty «Cybersecurity» should be based on the general concept of understanding of this concept in science and in legislation. Unfortunately, such an important document as the «Cybersecurity Strategy of Ukraine», approved by the Decree of the President of Ukraine of March 15, 2016 [13], does not contain an interpretation of the key concept. Therefore, it is worth resorting to the interpretation of cybersecurity by reputable scientists. Thus, O. Baranov interprets it as «such a state of protection of vital interests of the individual, society and the state in the conditions of use of computer systems and / or telecommunication networks, which minimizes their harm because of incomplete, untimely and unreliable information used; negative information impact; negative consequences of information technology functioning; unauthorized dissemination, use and violation of the integrity, confidentiality and accessibility of information» [14].

An undeniable advantage of this definition, we think, is its orientation on the humanistic nature, when the interests of the individual, and then of society and the state, come to the fore. This thesis is of fundamental importance, since all the activities of cybersecurity experts are methodologically connected not with their own technical issues, but with the protection of human rights through the full functioning of public and state institutions, the development of civil society.

Analysis of the training plans for cyber security specialists clearly shows that the humanization of education, including through the legal component, is not taking place. For example, only 2 ECTS credits (60 hours) are allocated to the bachelor's degree course at the «KPI», of which 36 work in the classroom.

In general, the list of disciplines of vocational and practical training for higher education graduates in the Cyber Security specialty looks somewhat unsystematic and detached from the needs of practice. Undoubtedly, such disciplines as «Introduction to cyber security», «Cyber security systems and technologies», «Security of operating systems and computer networks», «Internet resources security», «Information security management» are extremely important for the formation of a specialist. However, an expert

comment is needed, which makes sense to include in the category of vocational training subjects common to all engineers such as Algebra and Geometry, Differential Equations, which in essence should be presented in basic training subjects.

According to the Law of Ukraine «On Higher Education», the curricula for the preparation of higher education applicants must contain 25% of the disciplines of free choice of student. In the training of cybersecurity professionals, a block of vocational training courses should serve to build competencies for specializations in the perspective of future job positions. However, the courses offered are more likely to contribute to deepening their own mathematical training, they are almost identical to students studying in different specializations in the same specialty.

The curricula for the preparation of bachelors in the specialty «Cybersecurity» of the National Technical University «Kiev Polytechnic Institute» in general not only represent the legal disciplines, but also subjects of the documentary cycle, despite the widespread introduction in the organizations and institutions of the electronic document circulation. There are no educational programs or disciplines that would contribute to the spread of the global cybersecurity culture, macro- and microeconomic issues related to cybercrime technologies.

It is therefore logical to further analyze the qualification requirements for the competencies of cybersecurity professionals.

QUALIFICATION REQUIREMENTS FOR THE COMPETENCIES OF CYBERSECURITY PROFESSIONALS.

The dialectic of social development in all its historical stages is characterized by a recurring pattern: the progress of mankind is due to the permanent development of professionals, accompanied by the complexity of the requirements for their level of skill depending on the profession and the tools used. Another feature is the archiving of some professions and the emergence of new ones. This is most clearly seen in the field of information technology. The urgent need to prevent and combat cybercrime has made it necessary to establish qualifying requirements for those charged with this duty.

The question of the order, content, volume of qualification requirements for professionals of a certain profile was and remains in the field of view of scientists. Now thanks to the works of T. Kamenskaya, S. Melnik, Z. Podruchny,

V. Artificial and others bases for scientific substantiation of the qualification requirements for internal auditors, personnel of the water sector, translators, state security workers, etc. have been formed. Qualification requirements for experts in the organization of protection of information of restricted access were investigated by V. Koval, M. Logvinenko, P. Orlov, S. Shibalkin. The main attention was paid to the purely technical competencies of the engineering workers, who by their duties act within the limits of the Law of Ukraine «On State Secrets».

Despite the existence of certain well-established approaches to the universal algorithm for the formation of qualification requirements, there is reason to believe that the scientific foundations of their definition in relation to cybersecurity professionals have not been fully explored.

Therefore, the scientific substantiation of the qualification requirements for cybersecurity specialists on the basis of the competence approach is relevant.

Achieving this goal requires the following tasks: 1) determine the essence of the concept of «qualification requirements», its components; 2) establishing the degree of representation of the key concept regarding the competencies of cybersecurity professionals; 3) detailing of qualimetric indicators of activity of this category of specialists.

Qualification requirements for representatives of certain professions occupying certain positions are a kind of «phenomenon», since the concept's prominence gives the opportunity to consider it in a multidimensional projection.

First, they are a scientific concept that synthesizes the idea of an ideal object, which subsequently becomes the basis of the profession. Its creation is preceded by a thorough analysis of the sphere of activity, the role of the profession in society, the functions of a specialist in a certain position, integrative relations with other professional circles. Such analysis should be comprehensive and detailed and serve as a basis for normative implementation of qualification requirements at the level of state standards, which are approved by the relevant order of the Ministry of Labor and Social Policy of Ukraine in the context of qualification characteristics.

Therefore, *in the second sense*, the qualification requirements are a legally binding norm, which is obligatory for all personnel of organizations, institutions, institutions and so on. Currently, the qualification directory of posts is represented by 87 thematic issues, as well as four additional qualification

directories. The norms fixed in them are the basis for establishing employment relations, the basis for formulating the conditions for the selection of applicants for certain positions.

As stated in Issue 1 of the Handbook of Qualifying Characteristics of Workers' Occupations, it «contains indicators and features that bring it closer to methodological, methodological and regulatory practical aspects with national publications of this direction in other countries, and takes into account the recommendations of the executive bodies of the International Labor Organization ... » [15]. This practice is very important given the processes of globalization, the strengthening of the international labor market, the dynamic movement of workers not only within one country, but also the prospects of employment abroad or work for foreign organizations in remote access mode.

Third, qualification requirements are a guide for educational activities, as the training process for certain areas and specialties must be carried out in accordance with state standards. The peculiarity of the Ukrainian education system is that the trainees, along with a certain level of education, receive qualifications. The latter Law of Ukraine «On Higher Education» is defined as «the official assessment and recognition result obtained when an authorized institution has determined that a person has attained competencies (learning outcomes) in accordance with higher education standards, as evidenced by the relevant higher education document» [1] . In fact, state certification of graduates of higher education institutions can be considered in the aspect of testing their competencies for compliance with the qualification requirements for the specialty.

Fourth. In their applied sense, the «qualification requirements» are a concentrated indicator of the conditions presented to applicants for the position in the recruitment. Ideally, such requirements should clearly correlate with those qualifications that are enshrined at the level of state standards of professional activity, however, if they are absent or in the process of being drafted, the staffing unit can formulate them independently.

Based on the notion of the essence of the concept of «qualification requirements», let us analyze the extent to which it is detailed in relation to cybersecurity professionals.

From the standpoint of formulating the qualification requirements for the competencies of specialists of the specified category as a scientific concept, we note that they are mostly more or less developed for the segment of the

field of knowledge «Information Technology». This was facilitated by the scientific reconnaissance of V. Buryachko, I. Parkhomei, M. Stepanov, V. Tolubka [16]; I. Loginova [17], E. Skulish [18] and others. There are also some scientific papers that express ideas on the qualification requirements for lawyers specializing in cyber security. In particular, these problems are discussed in the publications of P. Bilenchuk [19], A. Wojciechowski [20], S. Demidyuk and V. Markov [21] and others.

It is characteristic that for the most part, scientific works are focused on becoming the basis for educational standards for training cybersecurity professionals, rather than being the basis for state standards of professional activity or serving to determine the competency requirements for personnel machines.

Therefore, our analysis of the representation of the qualification requirements for the competences of cybersecurity specialists has made it possible to establish that they are still being formed as a scientific concept. In a fragmentary way, these perceptions fall into educational standards, bypassing the component of state standardization, since no qualification requirements are presented in either the Classifier of Economic Activities or the National Classifier of Qualifications. We have allowed ourselves to use the word «fragmentary» because, depending on the areas of preparation of specialists to the standards, those elements of qualification requirements that are relevant to the specific direction, specialty and specialization of the higher education applicant fall.

Standardization of educational and educational programs in the field of cybersecurity training takes place at the level of higher education institutions licensed for this type of activity. Therefore, the qualification requirements are correlated with the components of the qualification characteristics, containing a list of typical professional tasks envisaged by job responsibilities, with the content of education within the elements «Must know», «Specialization», «Examples of work». The educational standards design algorithm provides for the formulation of qualification requirements based on typical tasks in a professional activity, taking into account the advanced nature of learning and the needs of practice that are constantly complicated. In this regard, the collaboration of research and teaching staff with future employers, which should be included in the design teams of designing educational standards, is of particular importance.

However, this issue requires separate research and may focus in another publication. At this stage, it is necessary to systematize existing approaches to articulating the qualification requirements of cybersecurity professionals. This task is fundamentally important, especially given the rather debatable opinion of renowned experts, which, unlike technical means, is the most complex and weakest chain in the cybersecurity system [876]. Therefore, it is in this plane that the spheres of activity of higher education institutions and personnel of organizations, institutions, institutions and business structures intersect to provide security in the computer space.

CONCLUSIONS.

In my opinion, the potential for improving the educational standards of cybersecurity professionals is to integrate theoretical knowledge and practical skills emerging in higher education with further work in specific sectors. Therefore, it would be possible to envisage specialization of cybersecurity specialists for further activities, especially in the following areas:

— *sphere of state power and administration* - introduction and maintenance of processes of secure e-government, state information resources, ensuring unimpeded work of information-analytical, statistical units, effective counteraction to cyber attacks on websites of state institutions and organizations, etc.;

— *security and defense* - activities in the context of ensuring national and information security in cyberspace; combating cybercrime, including cyber-terrorism, combating cyber-threats to military character, protecting the interests of the state by computer and technology warfare in information and hybrid wars; ensuring the operational state of cryptographic information security;

— *economic sphere* - prevention of cases of industrial espionage, theft of know-how, computer fraud with electronic payment documents, seizure of confidential economic data, illegal activities with payment and credit cards; theft of funds from electronic accounts, ordering goods and services at someone else's account, etc.

— *science and technology* - counteracting cyber-espionage, developing software that prevents intrusion into computer systems, spreading viruses, destroying databases and more.

The above list is not exhaustive, it can and should be supplemented. At the same time, it can be the starting point for developing the concept of cyber security education standardization, identifying specific specializations that will then be implemented through curricula.

With regard to the qualification requirements for the competences of cyber security professionals, it can be stated that the issue of selection, training and maintenance of appropriate qualification is one of the leading activities in the organization of combating cybercrime.

In Ukrainian reality, the needs of practice are often outstripped by theoretical developments and their legal consolidation in normative documents, including standardization. Quite demonstrative in this regard is the experience of forming in the structure of the National Police of Ukraine of the Department of Cyber Police. For us, this information is valuable from a scientific point of view, given that, unlike many other cases, these materials were in the public domain. Therefore, the need to select staff to replace the vacant positions in the said unit necessitated the formulation and announcement of qualification requirements for applicants for these positions.

REFERENCES:

[1] Pro vyshchu osvitu (Zakon Ukrainy), № 1556-VII vid 01 lyp. 2014 r.; v red. vid 30 lystopada 2016 r (2016) [*On Higher Education (Law of Ukraine), No. 1556-VII of 01 July 2014; in order. dated November 30, 2016*]. Retrieved from http://zakon2.rada.gov.ua/laws/show/1556-18. [in Ukrainian].

[2] Gordichuk, S. (2016) Stvorennia standartiv novoho pokolinnia u zabezpechenni yakosti medychnoi osvity [Creating new generation standards in quality assurance in medical education]. *Continuing professional education: theory and practice series: pedagogical sciences*, (46-47), 121–126. [in Ukrainian].

[3] Zhuravska, N. (2011) Reforma standartiv vyshchoi osvity [Reform of higher education standards]. *Youth and the market*, 8 (79), 27–31 [in Ukrainian].

[4] Kiselyova, O. I. & Yankova, O. V. (2013) Zmist ta zavdannia standartyzatsii vyshchoi osvity [Content and tasks of higher education standardization]. *Science and education*, 6, 90–95 [in Ukrainian].

[5] Streletz, S. (2012) Standarty fakhovoi pidhotovky u systemi vyshchoi osvity: napriamy vdoskonalennia [Standards for professional training in higher education: directions for improvement]. *Home school*, 1-2 (January-February), 17–22 [in Ukrainian].

[6] Terepishchiy, S. O. (2010) Standartyzatsiia vyshchoi osvity (Sproba filosofskoho analizu) [*Standardization of higher education (An attempt at philosophical analysis)*]. Kyiv: MP Drahomanov NPU [in Ukrainian].

[7] Pro zatverdzhennia pereliku haluzei znan i spetsialnostei, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity (postan. Kabinetu Ministriv Ukrainy), № 266 vid 29 kvit. 2015 r.; iz zmin. [*On approval of the list of branches of knowledge and specialties by which higher education applicants (Decree of the Cabinet of Ministers of Ukraine), No. 266 from April 29 2015*]. Retrieved from http://zakon2.rada.gov.ua/laws/show/266–2015–%D0%BF. [in Ukrainian].

[8] Pro vyshchu osvitu (Zakon Ukrainy), № 2984-III vid 17 sich. 2002 r. [*On Higher Education (Law of Ukraine), No. 2984-III of January 17, 2002*]. Retrieved from http://zakon5.rada.gov.ua/laws/show/2984-14. [in Ukrainian].

[9] Lipkan, V. A. & Dimchoglo, M. I. (2014) Konsolidatsiia informatsiinoho zakonodavstva Ukrainy [*Consolidation of information legislation of Ukraine*]. Kiev: O.S. Lipkan [in Ukrainian].

[10] Eksperty pro pidhotovku fakhivtsiv u sferi informatsiinykh tekhnolohii (2017) [*Experts on training of specialists in the field of information technologies*]. Retrieved from http://mon.gov.ua/usi-novivni/novini/2016/10/04/kruglij-stil-1016/. [in Ukrainian].

[11] Sumy State University. (2016). U SumDU vidkryly novu spetsialnist – «Kiberbezpeka» [*A new specialty was opened at SSU – «Cybersecurity»*]. Retrieved from http://sts.sumy.ua/education/u-sumdu-vidkrili-novu-spetsialnist-kiberbezpeka.html. [in Ukrainian].

[12] Semin, S. V. & Reznikova, O. O. (2016). Systema pidhotovky kadriv dlia syl bezpeky Ukrainy: problemy ta perspektyvy rozvytku [*Training system for Ukrainian security forces: problems and prospects*]. Kyiv: National Institute for Strategic Studies [in Ukrainian].

[13] Stratehiia kiberbezpeky Ukrainy: zatv. ukazom Prezydenta Ukrainy, № 96/2016 vid 15 berez. 2016 r. [*Ukraine's Cybersecurity Strategy: Approved. by decree of the President of Ukraine, No. 96/2016 from March 15, 2016*]. Retrieved from http://www.president.gov.ua/documents/962016-19836. [in Ukrainian].

[14] Baranov, O. A. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [About interpretation and definition of the term «cyber security»]. *Legal Informatics*, 2 (42), 54–62. [in Ukrainian].

[15] *Handbook of qualification characteristics of professions of workers.* (2019). Vyp. 1.: Profesii pratsivnykiv, shcho ye zahalnymy dlia vsikh vydiv ekonomichnoi diialnosti [*No. 1: Occupations of workers that are common to all types of economic activity*]. Retrieved from http://www.jobs.ua/ukr/dkhp. [in Ukrainian].

[16] Buryachok, V. L. (2013). Osnovy formuvannia derzhavnoi systemy kibernetychnoi bezpeky [*Fundamentals of formation of the state system of cyber security*]. Kyiv: NAU [in Ukrainian].

[17] Loginov, I. V. & Melnyk, D. S. (2011). Internet v OSD pidrozdiliv kontrrozvidky SB Ukrainy [*Internet in the OSD of the counterintelligence units of the Security Service of Ukraine*]. Kiev: Sciences edition of the National Academy of Security of Ukraine [in Ukrainian].

[18] Skulish, E. D. (2011). Faktory vplyvu na formuvannia systemy informatsiinoi bezpeky v Ukraini [Factors influencing the formation of the information security system in Ukraine]. *Information security of the person, society, state*, 2 (6), 22–26. [in Ukrainian].

[19] Bilenchuk, P. (2013). Doktrynalni zasady pidhotovky vysokokvalifikovanykh yurystiv novoi generatsii u XXI stolitti: zasoby, metody, tekhnolohii [The doctrinal principles of training highly qualified lawyers of the new generation in the 21st century: tools, methods, technologies]. Viche, (18), 7–9. [in Ukrainian].

[20] Wojciechowski, A. (2017). Mizhnarodne spivrobitnytstvo v borotbi z kiberzlochynnistiu [International cooperation in the fight against cybercrime]. *Law and security*, (4), 107–112 [in Ukrainian].

[21] Demedyuk, S. V. & Markov, V. V. (2015). Pidhotovka ta pidvyshchennia kvalifikatsii pratsivnykiv u sferi borotby z kiberzlochynnistiu [Training and advanced training of cybercrime workers]. *Pravo.Ua*, (1), 48–52. [in Ukrainian].