DOI: 10.2478/rpp-2019-0029

Postgraduate Student, **BOHDAN BRAIKO**
Khmelnytskyi National University
Address: 11 Instytutska St., Khmelnytskyi, 29016, Ukraine
E-mail: comprofped@gmail.com

COMPARATIVE PEDAGOGICAL ANALYSIS OF PROFESSIONAL TRAINING FOR MASTERS IN CYBERSECURITY IN UKRAINE AND THE UK

ABSTRACT

The article deals with the relevant problem of updating the system of graduate training (*master's degree*) *in Ukraine. It analyzes the ways of Ukraine's integration into the European Higher Education Area and the legal framework of higher education in Ukraine and the UK. It also presents a comparative pedagogical analysis of the features of professional training for Masters in Cybersecurity in different areas, as well as the structural, content, organizational and pedagogical principles of master programmes on cybersecurity at the universities of Ukraine and the UK. It is found that the most significant difference is the decentralized management of educational processes at the administrative level. The analysis of the legal framework of higher education shows that it is much better developed in Ukraine than in the UK due to the centralized management of education. The article proves that a significant difference between master programmes on cybersecurity in Ukraine and the UK is their level of specialization. The programmes on the investigation of computer incidents and information technology security are most prevalent at UK universities. It is specified that the number, list and names of educational courses differ significantly, which is explained primarily by the differences in the conceptual framework of the profession itself, the social needs of Ukrainian and British society in such specialists and the ways of promoting this profession in the labour market. Some positive aspects of the organization of master training in cybersecurity in the UK are emphasized. Some promising areas in professional training of Masters in Cybersecurity in Ukraine and the UK are singled out.*

Keywords**:** *cybersecurity, master programmes, specializations, structure, legal framework, comparative analysis, universities, the UK.*

АНОТАЦІЯ

У статті висвітлено актуальну проблему реформування системи професійної підготовки магістерського рівня в Україні. Проаналізовано шляхи інтеграції України в Європейський освітній простір, розглянуто законодавчо-нормативне забезпечення сфери вищої освіти України та Великої Британії. Здійснено порівняльно-педагогічний аналіз особливостей професійної підготовки магістрів з кібербезпеки за різними напрямами. Наведено порівняльний аналіз структурно-змістовних та організаційно-педагогічних засад навчання магістрів з кібербезпеки в університетах України й Великої Британії. З'ясовано, що на адміністративно-управлінському рівні найсуттєвішою різницею є децентралізація управління освітніми процесами. Аналіз законодавчо-нормативного забезпечення сфери вищої освіти дає підстави стверджувати, що в Україні, саме завдяки централізованому управлінню освітою, вона розвинута значно краще, ніж у Великій Британії. Визначено, що суттєвою відмінністю між освітніми програмами підготовки магістрів з кібербезпеки в Україні та Великій Британії є їх

рівень спеціалізації. Найбільшого поширення в університетах Великої Британії мають освітні програми з розслідуванням комп'ютерних інцидентів та безпеки інформаційних технологій. Зазначено, що кількість, перелік та назви дисциплін значно відрізняються, що пояснюється насамперед відмінностями у концептуальному баченні самої професії, суспільними потребами українського та британського суспільства у таких фахівцях та у можливостях реалізації цієї професії на ринку праці. Наголошено на окремих позитивних аспектах організації навчального процесу підготовки магістрів з кібербезпеки у британському досвіді, окреслено перспективні напрями підготовки магістрів з кібербезпеки в Україні і Великій Британії.

***Ключові слова*:** *кібербезпека, магістерські програми, спеціалізації, структура, законодавчо-нормативне забезпечення, порівняльний аналіз, університети, Велика Британія.*

INTRODUCTION

Such processes as updating the European-type system of step-by-step education, justifying its conceptual principles, modernizing graduate training (master's degree) in Ukraine and, therefore, searching for innovative and more effective ways to transform the structure and content of master's degrees in cybersecurity in the context of social integration processes are becoming more and more relevant. After all, the inconsistency between the areas, volume and quality of professional training to the needs and requirements of the labour market, the imperfection of the legal framework for master's education are the inhibiting factors in ensuring the social and economic stability of the country and competitiveness of the national higher education system in the world. The problem of reaching a compromise between the demands of society, the level of specialists' professionalism and their professional performance is becoming more and more acute.

However, the integration of Ukraine's education into the European higher education area requires that the history and the current state of master's education in well-developed countries should be studied in more detail and the promising areas and trends in this field should be identified. An objective scientific analysis of pedagogical achievements in foreign countries, in particular, the UK, can become a valuable source for understanding innovative ideas for elaborating a new strategy and developing the national system of master's education. Given the above, it is advisable to conduct a comparative pedagogical analysis on the features of professional training for Masters in Cybersecurity. Such an analysis covered different aspects, namely *regulatory, administrative and managerial, social, economic, systemic, conceptual and organizational*, to identify some common and different approaches to borrow positive achievements and prevent mistakes in the process of updating master's education in Ukraine. Consequently, the comparison of the UK experience, national realities and the justification of ways to find competitive alternatives will help to expand the boundaries of scientific knowledge about master's education, improve professional training for Masters in Cybersecurity and introduce new pedagogical realities.

THE AIM OF THE STUDY

The research aims to conduct a comparative pedagogical analysis of professional training for Masters in Cybersecurity in Ukraine and the UK.

THEORETICAL FRAMEWORK AND RESEARCH METHODS

The analysis of scientific, analytical and information sources, regulatory framework and pedagogical experience of professional training for Masters in Cybersecurity shows that there have been more Ukrainian studies on certain aspects of

master's training, including IT, in recent years (O. Baranov, V. Bykov, I. Diorditsa, D. Dubov, I. Dzhalladova, S. Melnyk, L. Zubyk et al.).

Ukrainian scholars have accumulated certain considerable experience in studying professional training of specialists in the UK (N. Avshenyuk, N. Bidyuk, O. Hohua, O. Pichkar, L. Pukhovska, V. Tretko et al.) The works of such foreign scholars as F. Edmundson, B. Joyce, D. Hamblin, M. Hollis, S. Paterson and K. Webb serve as a significant source for studying the UK educational system in terms of organizing professional training for masters.

RESULTS

A study of the scientific literature and the current legal framework show that a comparative analysis of the UK and Ukrainian master's education is complicated by their diversity and specificity. The comprehension and development of the UK experience and its adjustment to socio-political realities should take into account the pan-European trends and aim to solve the problematic aspects of master's education.

At the administrative and managerial level, the most significant difference is *the decentralized management of educational processes*. The UK higher education system is decentralized, while the Ukrainian higher education is subordinate to public authorities which are responsible for both management and monitoring of the quality of educational services. It remains unclear whether any of these systems is optimal for the Ukrainian educational environment since both of them have advantages and disadvantages. For one, the decentralized management and autonomy of higher education institutions in choosing educational priorities, on the one hand, promote certain competition between them and force rapid adjustment of educational programs to the needs of consumers of educational services and, on the other hand, make it impossible to conduct a nationwide monitoring and control of education quality and create common state educational standards.

A centralized approach to education management, on the one hand, ensures the integrity of master programmes on cybersecurity, the unity of requirements for the organization of the educational process and the qualification levels of graduates. On the other hand, a stable system for coordinating activities of higher education institutions and compulsory standards for the organization of the educational process, to a certain extent, deprive educational institutions of the opportunity to independently modify and supplement the content of educational programmes for specialists in a particular field, choose priority areas of educational activities, introduce new degree programmes and significantly change educational load, etc.

Considering the legal framework of master programmes on cybersecurity, the author of the article has focused on the following its components: international documents (the World Declaration on Higher Education for the Twenty First Century: Vision and Action, 1998; Convention on the Recognition of Qualifications concerning Higher Education in the European Region, 1997; Key Competences for Lifelong Learning: European Reference Framework, 2007); laws on higher education (Higher Education and Research Act, 2017; the Law of Ukraine "On Higher Education", 2014; the Higher Education Standard of Ukraine on the specialty No 125 "Cybersecurity", the field of knowledge No 12 "Information Technologies" for bachelor's education; National Cyber Security Strategy 2016-2021 (2016); the Presidential Decree "On Ukraine's Cybersecurity Strategy" (2016); the Law of Ukraine "On Basic Principles of Assuring Cybersecurity of Ukraine", 2017); regulatory documents of the UK and Ukrainian universities, defining general provisions for admission, awarding of qualifications, monitoring of education quality, as well as educational and professional programmes, module descriptions, etc.

The analysis of *the legal framework* of higher education shows that it is much better developed in Ukraine than in the UK due to the centralized management of education. The educational process in the UK is legally regulated by relevant legislative acts (the Education Reform Act, 1988; the Further and Higher Education Act, 1992; the Higher Education Act, 2004; the Higher Education and Research Act, 2017). However, the Department for Education has the authority to directly implement them. Decisions on the activities of certain higher education institutions are made at the level of professional organizations and associations, unions of universities, etc. The international office for European Higher Education Policy in the interest of the UK's higher education is the central body for coordinating information gathering and policy-making in higher education, internationalization and European policy for UK higher education institutions.

It must be noted that a higher education institution in the UK acts an independent legal educational institution and has a board or governing body, which is responsible for determining the strategic areas in the institution's development, controlling its financial position and ensuring effective management. In the UK, there is no single master programme of professional training for Masters in Cybersecurity (120 different programs in total). Quality is a must in this context. Every educational institution is primarily responsible for maintaining the quality of education and the standards of qualifications, which are controlled by the independent Quality Assurance Agency for Higher Education (QAA) (Quality Assurance Agency, 2004).

In Ukraine, educational activities in higher education institutions are organized following the Laws of Ukraine "On Education", "On Higher Education", Higher Education Standards and other applicable regulatory documents.

Master programmes are developed in accordance with the Law of Ukraine "On Higher Education" (2014), resolutions of the Cabinet of Ministers of Ukraine "On the Approval of the National Qualifications Framework" (2011), "On the Approval of Licensing Conditions for Educational Activities in Educational Institutions" (2015), methodical guidelines for the development of degree programmes.

However, the Ukrainian experience in training Masters in Cybersecurity shows that the legislative basis in this field still needs updating and improving. Indeed, it is essential to develop the Higher Education Standard of Ukraine on the specialty No 125 "Cybersecurity" for master's degrees (*Pro zatverdzhennia standartu*, 2018).

The first step towards the modernization of Ukraine's higher education in the context of introducing the specialty No 125 "Cybersecurity" of the IT industry was the adoption of the Decree of the Cabinet of Ministers of Ukraine "On the Approval of Knowledge Areas and Specialties for Higher Education" (2015). According to this document, the list of branches of knowledge and specialties was adjusted as follows: the knowledge area No 1701 "Information Security" disappeared, including specialties No 170101 "Information and Communication Systems Security", No 170102 "Systems of Technical Security of Information" and No 170103 "Information Security Management". The knowledge area No 12 "Information Security" also includes the specialty No 125 "Cybersecurity". The type(s) of activities should be approved by the appropriate state body that ensures the fulfilment of national security tasks, in agreement with the Ministry of Education and Science.

It is also necessary to pay specific attention to a comparative analysis of the structural, content, organizational and pedagogical principles of professional training for Masters in Cybersecurity at the universities of Ukraine and the UK. It is found that,

nowadays, the leading trends in the national education of Ukraine and the UK include the compliance with the pan-European requirements, which implies improving the higher education system, implementing the ideas of the Bologna process, updating the goals and content of professional training for Masters in Cybersecurity. A common approach is the desire of both countries to create a system of master's education based on the combination of national traditions with the requirements of European integration processes and challenges of the globalized world (Vitvytska, 2004, pp. 69–71). The ability to synthesize these two aspects is aimed at preparing a competitive cybersecurity specialist of the new generation, who can perform professional activities under the conditions of information society and market economy.

As regards the creation of degree programmes, the UK universities have more freedom in defining their content, although the current tendency to integrate into the European Higher Education Area has shown the expediency of coordinating and standardizing such programmes. However, all documents used to organize the educational process of professional training for Masters in Cybersecurity have clearly defined strategic goals and objectives (Quality Assurance Agency, 2010). They are coordinated with Universities UK (UUK), funds for strengthening competitiveness, the Association of Colleges and the National Board Certification under professional standards. The result of such activities is the prompt adjustment of standards following the requirements of the labour market. In Ukraine, unfortunately, such an operational adjustment of standards is not yet available.

Besides, the Ukrainian education system is characterized by low *academic mobility of students*. Practice shows that students usually continue their master studies in the same higher education institution where they obtained a bachelor's degree. Still, students of other universities with the corresponding bachelor's degree can be admitted, too. In the UK, by contrast, masters programmes operate independently of undergraduate programmes and provide one to two (at least three) years of study for students who have already obtained a bachelor's degree in a relevant field. At the UK universities, those who wish to be enrolled in master programmes on cybersecurity do not need to have a bachelor's degree in this field. As one can see, the UK approach to organizing admission to the master's programmes in cybersecurity differs from the Ukrainian one.

All of the factors discussed above (education management system, legal framework, student mobility) directly influence the organization of master programmes on cybersecurity in higher education institutions in both countries.

A significant difference between master programmes on cybersecurity in Ukraine and the UK is *their level of specialization*. In the UK, the system of professional training for Masters in Cybersecurity combines broad-based and narrow-based programmes which provide specialized training in various fields.

The analysis of more than 100 master programmes in the field of information security in different higher education institutions in the UK reveals the following training areas: master programmes on computer security focused on studying methods and tools of computer security: Cyber Security, Computer Security, Ethical Hacking for Computer Security.

Master programmes in the field of information technology security focused on studying the ways and methods of assuring integrated security in various information systems (business systems, finance) and technologies: Information Security, Information Security Systems with Business Finance, Information Security Systems.

Master programmes in the field of investigating computer incidents are aimed at training future specialists to analyze and examine computer systems to obtain evidence that

can be used in criminal processes, such as Computer Forensics and Security, Computer Forensics, Accounting Information Systems and Computer Forensics.

Master programmes in computer network security which include basic network security technologies, local and global network security protocols, such as Internet Computing and Network Security, Computer Network Security, Advanced Computing (Internet Technologies with Security).

Master programmes in the field of information security management which provide the necessary theoretical and practical skills in developing a security policy, security standards, organizational aspects of information security: Information Security and Information Security Management, Information Security and Information Technology Management, Information Security Management.

Upon completion of these programmes, one can obtain bachelor's and master's degrees in arts, science or engineering"; a master's degree in law; a master's degree in philosophy. Also, after obtaining a bachelor's degree, there is an opportunity to obtain PgCert or PgDip.

In the UK, the most common are master programmes on information technology security (33 %). There is a certain decrease in the number of master programmes on the investigation of computer incidents (17 %) and IT legislation (9 %). It must be noted that the vast majority of these programmes result in a master's degree in science, except for the areas of legislation in the field of information technology and information security management, which allow one to obtain a master's degree in laws and humanities.

Besides, the UK is the only country where students, after successful completion of their studies, have the opportunity to obtain an academic master's degree in information security. There are also a large number of different programmes on the legislation in the field of information security.

In Ukraine, such specializations are not common, although several such programmes already exist in Ukrainian higher education institutions (Security of State Information Resources; System of Technical Protection of Information and Automatization of Its Processing; Security of Information and Communication Systems; Administrative Management in the Field of Information Security; Management of Information Security; Mathematical Methods of Cybersecurity; Technical Systems of Information Security and Cybersecurity; Information Security and Cybersecurity).

The analysis on educational opportunities of professional training for Masters in Cybersecurity shows that 27 higher education institutions offer such training in Ukraine (46 programmes) and 69 higher education institutions – in the UK (120 programmes). In Ukraine, taught master programmes are allocated 90 ECTS, whereas research master programmes – 120 ECTS. The programmes can last year and a half or two years. In the UK, master programmes on cybersecurity are allocated 180 CATS, that is equivalent to 90 ECTS and last one or two years.

In Ukraine, the top five higher education institutions, which provide training in cybersecurity, include Kharkiv National University of Radio Electronics, National Aviation University, Ihor Sikorsky Kyiv Polytechnic Institute, Lviv Polytechnic National University, Taras Shevchenko National University of Kyiv.

Top UK universities offering master programmes on cybersecurity include the University of York, University of Birmingham, Royal Holloway University of London, University College London, University of Southampton, Newcastle University, University of Surrey, University of Warwick.

This research conducts a comparative analysis of master programmes in cybersecurity offered by Kharkiv National University of Radio Electronics (4 master programmes) (Kharkivskyi natsionalnyi universytet radioelektroniky, 2018) and Universities of Southampton (2018) and Birmingham (2018).

Master programmes on cybersecurity at Universities of Southampton and Birmingham are among those 25 MSc programmes on cybersecurity, which have been fully certified under the standards of a certified master of the National Cyber Security Centre (NCSC) (2019). NCSC certified master's degree programmes help universities attract the best students from all over the world who can make more informed choices about the degree programme.

In accordance with the requirements of the Bologna Declaration, the educational process in both institutions is based on credit-based modular learning. In Ukraine, master programmes on cybersecurity consist of 13–15 academic subjects, including 9–10 compulsory subjects (modules) allocated 65–70 ECTS (65–78 %) and 4–5 optional subjects allocated 22–25 ECTS (25–30 %). Compulsory professional subjects are the following: "Fault-Tolerant Computer Systems and Networks", "Modelling and Evaluation of the Effectiveness of Information Security Means", "Application of Design Diversity in Cryptography and Coding", "Monitoring and Audit of Information and Communication Systems", "Technologies of Administration and Operation of Protected Information and Communication Systems", "Methods of Creation and Analysis of Cryptosystems", "Administration and Protection of Databases", "The Analysis System and Ethical Hacking", "Information Security of Telecommunications and Cloud Technologies", etc.

The optional subjects are "Methods of Cryptanalysis", "Design of Mobile Technologies", "Methods for Protection of Decentralized Systems and Networks", "Theory of Distributed Information Resources and Protection of Databases". Also, students have the opportunity to choose one subject from humanities and socio-economic subjects, namely "Philosophical Problems of Scientific Knowledge", "Professional Foreign Language", "Pedagogy of Higher Education", "Intellectual Property".

Taught master programmes are allocated 90 credits. At the same time, 60 credits are allocated for compulsory and optional modules, 15 credits – for teaching placement and 15 credits – for master's thesis.

At University of Southampton (2018), master programmes on cybersecurity contain only 7 compulsory modules ("Security of Cyber-Physical Systems"; "The Basics of Cybersecurity"; "Network and WEB Security"; "Software Security"; "Cybercrime"; "Project Preparation"; "Cryptography") and three optional modules (only one can be chosen) ("Project Management and Software Development", "Machine Learning Technologies", "Criminal Behaviour – Applied Prospects"). The total number of credits allocated to this master programme is 180 CATS, which corresponds to 90 ECTS (Vitvytska, 2004). It must be noted that 105 CATS / 52.5 ECTS are allocated for compulsory modules, 15 CATS / 7.5 ECTS – for optional modules and 60 CATS /30 ECTS – for master's thesis. This programme offers an interdisciplinary approach to cybersecurity that covers not only technical subjects but also aspects of criminology, risk management, law and the social sciences providing learning outcomes highly valued by leading employers.

At University of Birmingham (2018), master programmes on cybersecurity (MSc Cybersecurity) contain 6 compulsory modules (60 CATS /30 ECTS) ("Cryptography"; "Security Systems Design"; "Forensic and Malware Analysis"; "Network Security"; "Secure Programming"; "Secure System Management"), 11 optional modules ("Advanced

Cryptography"; "Compilers and Languages"; "Computerized Verification"; "Hardware and Embedded Systems Security"; "Intellectual Analysis of Data"; "Mobile and Cloud Computing"; "Networks"; "Operating Systems" (60 CATS /30 ECTS can be chosen) and a master's research project (60 CATS /30 ECTS).

This programme allows students to gain knowledge and experience to evaluate, design and build secure computer systems and processes. It covers the theory and practice of designing and creating secure systems and provides solid knowledge about cryptography, network security and secure programming, as well as additional knowledge about hardware and embedded systems security, operating systems, incident management and forensics. Masters gain hands-on experience of working with technologies and tools for creating online software.

Optional subjects are important components of curricula. The number, list and names of educational courses differ significantly, which is explained primarily by the differences in the conceptual framework of the profession itself, the social needs of Ukrainian and British society in such specialists and the ways of promoting this profession in the modern (global) labour market. Despite the almost perfect theoretical aspect of Ukrainian master programmes, they still have some practical disadvantages. Indeed, the main one is the limited right of students to choose optional subjects (which are usually chosen by the faculty). Instead, Master students in the UK are entitled to choose their subjects. Therefore, it is crucial to provide Ukrainian students with the right to choose academic subjects, which, could be a significant step in promoting national professional training not only in Ukraine but also abroad.

Comparing the volume of master programmes, it can be concluded that the one-week load for a Master student in the UK is lower than in Ukraine (15-16 academic hours, sometimes less in comparison with 18–20 academic hours). This is explained, first of all, by the fact that the content of taught master programmes on cybersecurity both in the UK and in Ukraine provides intensive theoretical and practical independent training.

It must be noted that future masters in both countries work on long-term (semester-long) individual research projects (master's theses, dissertations), present their results in the form of scientific articles, reports at conferences, participation in international projects, thereby developing research skills and strengthening theoretical and research training in the field of specialization. A master's thesis in Ukrainian higher education institutions involves analyzing and theoretically elaborating (modelling and studying processes) topical issues, problems of the current state and development of the world community and international relations.

At UK universities, a master's thesis is allocated a significant part of study hours (150–200 hours), which implies using the resources of universities and relevant teaching and learning environment. A master's research in cybersecurity is the optimal condition for developing their research competence and should be focused on obtaining additional professional knowledge and skills aimed at developing research skills in the field of professional specialization. Students have access to a large number of full-text online cybersecurity resources in various UK libraries. All the work on a master's thesis is based on strong links with leading IT companies, both in the UK and in other countries, including Cisco, Microsoft, Oracle, IBM, Agilent Technologies, Erlang Solutions, Hewlett Packard Laboratories, Ericsson, Nvidia and Nexor. In Ukraine, unfortunately, the opportunities for realizing the research potential of undergraduates are very limited technically, methodologically and practically.

In the UK, master research projects allow students to demonstrate professional competence in solving the difficult software-related task and apply the acquired knowledge. Project topics are offered by university teachers or students' original ideas are used. Projects are of practical importance and are often implemented in the industry with employment opportunities for graduates. Students work on their projects independently under the guidance of a university teacher. It must be noted that such consultations are allocated 10 hours. It is also possible to organize a one-week project course with compulsory attendance. At different universities, master projects can contain from 15000 to 40000 words or from 45 to 80 pages.

There are great opportunities for Ukrainian Masters in Cybersecurity to develop professional skills and gain professional experience abroad. However, the state does not have time to respond to this situation, thereby losing its authority in the world and diminishing the capabilities of such specialists. Therefore, the integration into European Professional Associations and the European Higher Educational Area, the strengthening of legal support for professional activities and the reconsideration of training content in line with world experience should be the most important areas in the development of master programmes on cybersecurity in Ukraine.

CONCLUSIONS

Therefore, it must be noted that the UK and Ukrainian master programmes on cybersecurity are significantly different. At the same time, they are similar in development trends. First of all, the difference is in the content of taught master programmes at the UK and Ukrainian higher education institutions. Master's degrees in Cybersecurity are primarily focused on the national (regional) labour market, comprehensive development of the future specialist's personality and the cultivation of professional qualities. In the UK, such training is research-driven and focused on the global labour market. Given the above, it is advisable to review the content of master's degrees in Cybersecurity, in particular, its orientation on professional and research training, taking into account the most innovative achievements of foreign experience, in particular, the UK one. An important mission of Ukrainian higher education institutions is to enhance the process of teaching professional subjects and specialized subjects related to them, to provide students with modern educational and methodical materials and involve foreign specialists in the teaching process. It is also worthwhile to foresee the broad opportunities for internships abroad, as is done at leading universities in the UK.

Further research should be focused on the study of content characteristics of master programmes on cybersecurity in the EU.

REFERENCES

1. HM Government. (2016). *National Cyber Security Strategy 2016 to 2021*. Retrieved from https://www.gov.uk/government/publications/national-cyber-security-strategy-/2016-to-2021.

2. Kharkivskyi natsionalnyi universytet radioelektroniky. (2018). *Mahistr. 125 – Kiberbezpeka*. Vziato z https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/magistr-125-kiberbezpeka.

3. *National Cyber Security Centre (NCSC)*. (2019). Retrieved from https://www.ncsc./gov.uk.

4. Pro zatverdzhennia standartu vyshchoi osvity za spetsialnistiu 125 "Kiberbezpeka" dlia pershoho (bakalavrskoho) rivnia vyshchoi osvity. №1074. (2018).

5. Quality Assurance Agency. (2004). *Code of practice for the assurance of academic quality and standards in higher education. Section 1: Postgraduate research programmes*. Retrieved from http://www.qaa.ac.uk/Pages/default.aspx.

6. Quality Assurance Agency. (2010). *Master's degree characteristics*. Retrieved from http://www.qaa.ac.uk/Pages/default.aspx.

7. The European Education Directory. (2014). *England higher education system*. Retrieved from http://www.euroeducation.net/prof/ukco.htm.

8. University of Birmingham. (2018). *Cyber Security Masters/ MSc*. Retrieved from https://www.birmingham.ac.uk/postgraduate/courses/taught/computer-science/cyber-security.aspx

9. University of Southampton. (2018). *MSc Cyber Security*. Retrieved from https://www.ecs.soton.ac.uk/programmes/msc-cyber-security.

10. Vitvytska, S. S. (2004). Teoretychni zasady pidhotovky mahistriv v umovakh stupenevoi pedahohichnoi osvity. *Visnyk Zhytomyrskoho derzhavnoho universytetu imeni Ivana Franka*, 19, 69–71.