DOI: 10.3189/2308-4081/2020-10(4)-5

Doctor of Science in Pedagogy, Full Professor, **VITALIY TRETKO**
Khmelnytskyi National University
Address: 11 Instytutska St., Khmelnytskyi, 29016, Ukraine
E-mail: tretko@hotmail.com

PhD in Engineering, Associate Professor, **YURIY VASHKURAK**
Lviv Polytechnic National University
Address: 12 Stepan Bandera St., Lviv, 79000, Ukraine
E-mail: yu.pawluk@gmail.com

PhD in Pedagogy, **ARTUR GORBENKO**
Hetman Petro Sahaidachnyi National Army Academy
Address: 32 Heroi Maidanu St., Lviv, 79026, Ukraine
E-mail: arturgor2764@gmail.com

PROFESSIONAL CERTIFICATION AND ADVANCED TRAINING OF CYBERSECURITY PROFESSIONALS IN THE UK

ABSTRACT

The article deals with professional certification and advanced training of cybersecurity professionals in the UK. It shows that researchers in the UK, as well as in Western Europe, are debating the meaning of "recognition", "accreditation", "certification" and "licensing" of professional qualifications. The reason for such an interest is the legitimate try to implement the employment freedom principle, the specific need to make full use of professionals' working capacity and professional competence and the promotion of mobility and exchange in the European space. The article indicates that professional recognition of higher education qualifications in the UK somewhat differs from that in Western Europe. Professional recognition lies in obtaining the status of a certified professional in the field of cybersecurity under international standards, rather than obtaining an appropriate academic degree. The article proves that certification and advanced training of cybersecurity professionals in the UK is provided at the level of universities, international organizations. Besides, they take various forms (*mainly online learning*) *on a paid basis, differ in the duration of the study and the content of courses. The following structures and companies are considered as most prestigious for employment* (*internship*): *"Accenture", "Canary Wharf", "Indonesian Ministry of Finance", "JP Morgan", "IBM", "Ministry of Defence", "Royal Mail", "Singapore Police", "CISCO", "Facebook" and many others. Importantly, they put forward significant demands on the certification of professionals. The recognition of cybersecurity professionals' qualifications lies in two forms (state and certified). Certification takes place in the Academic Centres of Excellence in Cyber Security Research, the National Cyber Security Centre, as well as in public and private companies and international organizations. They create opportunities for obtaining the status of a Master in Cyber Security, a certified cybersecurity engineer, a certified IT support professional.*

Keywords**:** *certification, advanced training, cybersecurity professional, the UK, cybersecurity.*

АНОТАЦІЯ

Стаття присвячена професійній сертифікації та підвищенню кваліфікації фахівців з кібербезпеки у Великій Британії. З'ясовано, що у Великій Британії, як і в країнах Західної Європи, вчені дискутують щодо змісту понять «визнання», «акредитація», «сертифікація», «ліцензування» професійної кваліфікації фахівців. Причина такої зацікавленості полягає не лише в закономірному бажанні втілити у життя принцип свободи працевлаштування, але й у конкретній потребі повного використання працездатності та професійної компетентності фахівців, поширення процесу мобільності та обміну у європейському просторі. Зазначено, що професійне визнання кваліфікацій у вищій IT-школі Великої Британії має дещо інший характер, ніж у країнах Західної Європи. Професійне визнання – це не отримання відповідного академічного ступеня, а, насамперед, отримання статусу сертифікованого фахівця в галузі кібербезпеки відповідно до міжнародних стандартів. Визначено, що сертифікація та підвищення кваліфікації фахівців з кібербезпеки забезпечується на ріні університетів, відомих міжнародних організацій, відбувається у різних формах (*переважно онлайн навчання*), *на платній основі, різна за тривалістю навчання і змістовим наповненням курсів. Найбільш престижними для працевлаштування* (*стажування*) *є структури й компанії: «Accenture», «Canary Wharf», «Indonesian Ministry of Finance», «JP Morgan», «IBM», «Ministry of Defence», «Royal Mail», «Singapore Police», «CISCO», «Facebook» та ін., які висувають значні вимоги до сертифікації фахівців. Процедура визнання професійної кваліфікації фахівців у галузі кібербезпеки має дві форми – державну й сертифікатну. Сертифікація відбувається в Академічних центрах досконалості досліджень кібербезпеки, Національному центрі кібербезпеки, а також у державно-приватних структурах, міжнародних організаціях, що створюють можливості для одержання статусу сертифікованого магістра з кібербезпеки, сертифікованого інженера з кібербезпеки, сертифікованого професіонала з інформаційного забезпечення.*

Ключові слова: *сертифікація, підвищення кваліфікації, фахівець з кібербезпеки, Велика Британія, кібербезпека.*

INTRODUCTION

To begin with, researchers in the UK, as well as in Western Europe, are debating the meaning of "recognition", "accreditation", "certification" and "licensing" of professional qualifications. The reason for such an interest is the legitimate try to implement the employment freedom principle, the specific need to make full use of professionals' working capacity and professional competence and the promotion of mobility and exchange in the European space. Furthermore, there is no single approach to interpreting the terms "recognition" and "accreditation". In some cases, they can be interchangeable and synonymous. In educational terms, recognition implies that a certain degree programme, institution or person meets certain requirements and quality standards. Besides, the main focus is on the availability and provision of appropriate quality for potential customers (students, businesses, NGOs) or society as a whole.

In 1994, the European Commission identified 4 types of "recognition" for professional and academic purposes: de jure professional recognition; de facto professional recognition; general academic recognition; academic recognition by substitution. The 1997 Convention on the Recognition of Qualifications concerning Higher Education in the European Region defines "recognition" as formal confirmation of qualification by a

competent authority with access to education or employment. Qualification is considered in two aspects: qualification as the level of education obtained; qualification as a degree, diploma or certificate issued by a competent authority, which indicates successful completion of the relevant curriculum (Council of Europe, 1997).

Professional recognition of higher education qualifications in the UK somewhat differs from that in Western Europe. Professional recognition lies in obtaining the status of a certified professional in the field of cybersecurity under international standards, rather than obtaining an appropriate academic degree.

THE AIM OF THE STUDY

The article aims to analyze and justify the features of professional certification and advanced training of cybersecurity professionals in the UK.

THEORETICAL FRAMEWORK AND RESEARCH METHODS

According to the Skills Framework for the Information Age (SFIA), certification is diversified by three levels of competences: chartered professional, incorporated expert, professional expert. The main certification criteria include the following: autonomy in performing various complex tasks; business and project skills; experience; critical thinking; corporate management skills, responsibility. They confirm one's ability to use and implement technologies, apply information and/or cybersecurity tools, employ security mechanisms in decentralized systems, as well as effective means of limiting the risks of creating and using cryptocurrencies, smart contracts, blockchain technologies (SFIA, 2020).

Certification is one of the most optimal ways of developing and training IT professionals who face global cybersecurity threats and strive to change or start their career in cybersecurity. The certification confirms knowledge of key cybersecurity concepts, standards, guidelines and practices.

It is professional organizations/associations that enable the content-related development of curricula on IT, monitor the provision of future professionals with practical experience, carry out certification and determine the necessary programmes of certification and advanced training (The Chartered Institute for IT Professionals, 2020).

There is the ranking of the top 15 international IT certificates that allow graduates and professionals to be competitive in the global IT labour market, including in the field of cybersecurity. Listed below are some of them:

– the certified ethical hacker (CEH) certification allows professionals responsible for online data security to prove their ability to test security with hacking tools and techniques;

– CISSP (Certified Information Systems Security Professional) is an independent information security certification awarded by the International Information System Security Certification Consortium;

– the CRISC certification enables cybersecurity professionals to conduct a risk assessment, as well as implement, develop and maintain information system control tools;

– the AWS certification provides cybersecurity professionals with the experience of developing and maintaining Amazon cloud-based applications and enables them to effectively use AWS software developer tools to optimize application performance (New Horizons, 2019).

The National Cyber Security Center* (*NCSC, part of GCHQ*)*'s Certified Cyber Professional* (*CCP*) *scheme has been developed in collaboration with government agencies, academia, industry, certification bodies and developers of the previous framework (CESG, CLAS and CREST) (see Fig. 1). The document contains updated terminology, requirements

for the level of professional competences, certification procedure. The following three certification bodies designated by the NCSC manage the certification process: APM Group, BCS, The Chartered Institute for IT Professionals, the IISP, RHUL та CREST Consortium. They evaluate applications, determine the previous level of professional competence (knowledge, skills), involve leading IT professionals in training sessions, organize testing and develop certificates (indicating the level and status) (The National Cyber Security Center, 2018).

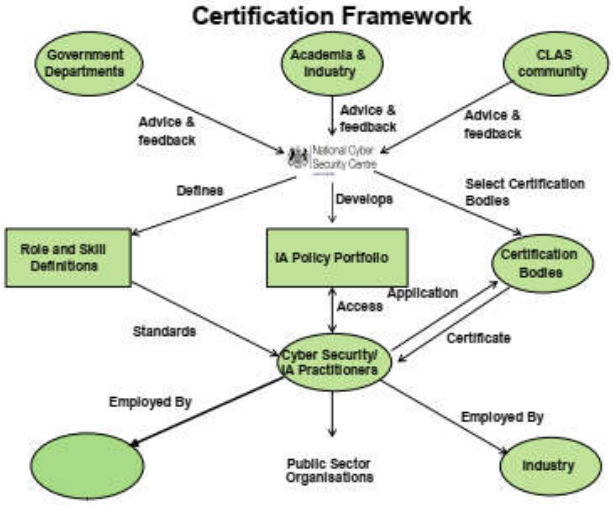

Fig. 1. The National Cyber Security Center (NCSC, part of GCHQ)'s Certified Cyber Professional (CCP) scheme

Source: The National Cyber Security Center. (2018). *Certified professional scheme*. Retrieved from https://www.ncsc.gov.uk/information/about-certified-professional-scheme.

The main goal of the scheme is to increase the level of professionalism in the field of cybersecurity under the British Cyber Security Strategy, as well as to eliminate contradictions between the needs of the industry in highly qualified professionals and ineffective mechanisms for quality training in higher education and certification and advanced training centres. One could observe how particularly acute is the need for public data protection and information risk management in the public sector. Subsequently, the complexity of the skills and competences needed by such professionals continues to grow (Cabinet Office, 2011). The main objective of the scheme is to involve cybersecurity and information support practitioners in an effective certification and knowledge examination process. Accordingly, the International Organization for Standardization (ISO) developed the ISO 1724 standard "Conformity assessment – General requirements for bodies operating certification of persons" (ISO, 2012). The important components of the scheme are a list of skills grouped according to their levels of development and professional functions (roles). These roles include the following: accreditor, security engineer, cryptographer, security auditor, IT security engineer, system manager, security management system engineer, security and information risk advisor, chief information security and cybersecurity officer.

Given the conditions of informatization, it has become essential to develop online certificate programmes which reflect the real quality of the acquired knowledge and experience, enable employers to select the best cybersecurity professionals, provide certain benefits in employment and create favourable career prospects. Besides, such programmes make it possible to increase the status and demand for cybersecurity professionals and indicate their determination. The advantages of online certificate programmes are as follows: speed of training and certification (depending on one's capabilities, such as free time, Internet access, determination, one can complete training in a short time and obtain a certificate after receiving a certain number of points); flexibility (one can train at any time); territorial independence; comfortable learning conditions; interactive communication.

Research methods include systematization, generalization, analysis, synthesis.

RESULTS

Listed below are the most well-known certification cybersecurity programmes in the UK.

Cyber Security Certification Programme with Job Guarantee has been developed by CompTIA Network +. It is an international (six-month, part-time) programme, which allows one to become the certified ethical hacker (CEH). The programme provides students with the basic skills and knowledge they require for a successful career in cybersecurity and good employment opportunities. It also involves practical training and participation in laboratory classes with a team of expert trainers who have experience in the field for over 15 years. Importantly, the programme prepares future professionals for subsequent employment (partial or full). The forms of learning include the following: practical training in the workplace; laboratory training; seminars; interviews; meetings with employers. It must be noted that the course on e-career within this programme has helped more than 4,000 students to become certified professionals and successfully start their careers in IT and cybersecurity. Many of them work in the world's largest companies such as Apple, AT&T, HMRC, Exponential-E, Rackspace and Swiss Quote in the positions of cybersecurity analysts, ethical hackers, incident handlers, web application experts, network administrators.

One should also pay particular attention to *the certified cybersecurity professional* (*CCS-PRO*) *training course.* The programme focuses on understanding the importance of cybersecurity, identifying potential cyber threats to businesses and business organizations and providing relevant recommendations to reduce cyber risks. Future professionals have the opportunity to study the motives and tools of hackers, phishing and participate in discussions on other areas of cybersecurity (threats related to social media, the Internet and mobile devices).

The first module of the program is aimed at a comprehensive understanding of cyber threats affecting business in today's technological world (hacking, phishing, web security, social media, mobile devices, spyware, malware, physical security). The second module involves developing the skills one needs to prevent cyber-attacks at the enterprise (password protection, encryption and two-factor authentication,). After completing the programme, students are well informed and understand how to combat cybersecurity threats and prevent malicious attacks. The third module seeks to improve students' skills in detecting unauthorized access or security threats, which will lead to data or financial loss and serious damage to the enterprise. Also, students work with the samples of malware and vulnerabilities detected by ethical hackers and often corrected during testing. Although ethical hackers tend to use the same tools and methods used by cybercriminals and attackers, ethical hackers have the permission of an authorized party to commit hacking. Ethical

hackers, commonly referred to as penetration testers or white-hat hackers, are experienced professional hackers who identify and exploit vulnerabilities in target systems or networks.

Also, this programme offers modules developed together with EC-Council at the core, advanced and expert levels. The most common dual certificates offered by the programme are SANS/GIAC Penetration Tester Certification (GPEN), Offensive Security Certified Professional (OSCP), CREST Certification, Foundstone Ultimate Hacking Certification, Certified Penetration Testing Consultant (CTPC), and Certified Penetration Testing Engineer (CPTE). Certificates qualify a professional as a certified ethical hacker and provide various benefits since it helps one to understand the risks and vulnerabilities affecting the activities of companies and businesses. One can obtain such qualifications in training centres throughout the UK. Interestingly, exams are conducted by independent experts, and professional associations issue certificates to their members. Such a distributed system acts as a guarantee of independent confirmation of professional skills and competences.

The EduCBA advanced training course is designed to help software professionals to gain an overview of hacking techniques with practical examples. It provides insights into hacking strategies, research configurations, topologies, network types and improves ethical hacking skills. In turn, future professionals can enhance their knowledge of cybersecurity and Internet security and appropriate skills. The course contains 105 lectures with 19-hour HD video. Learning tools involve the latest IT and hacking technologies, such as Port Scanning, ICMP Sweep / Scanning, ICMP Echo-fping, gping, Nmap for UNIX, Pinger Software-Rhino, Ping Sweep for Windows, NetBIOS Hacking, Internet Application Security and Vulnerability. Besides, students learn attack techniques, types of attacks (passive, active, distributed, insider, closed, phishing, kidnapping, fake, buffer overflow, password and passwordless), methods of user identity defence (social media, profiles, privacy settings, use of multiple passwords, phishing emails, HTTPS for online transactions), ways of reducing risks of online theft identification, features of phishing (and anti-phishing. Table 1 shows the scheme of professional development for cybersecurity professionals.

Table 1

The Scheme of Professional Development for Cyber Security Professionals in the UK

Academic (fundamental) profession-oriented training			
Universities			
Duration		Two years	Three (four) years
Qualification level		Master of Science	Bachelor of Engineering
Professional (practical) training			
Gaining practical experience		Independent work	
Acquiring professional and practical knowledge		Training under individual programmes	
Acquiring professional skills		Internships	
Professional certification and advanced training			
Professional functions	*Complex projects management*	*Team management*	*Expertise*
Educational level	Chartered professional	Incorporated professional	Professional expert

Source: National Cyber Security Centre. (2020). *CIISec, CREST and RHUL Consortium* (*CCP*). Retrieved from https://www.ncsc.gov.uk/evaluation-partner/ciisec-crest-and-rhul-consortium-ccp

A professional must have an appropriate diploma of an accredited higher education programme) and work experience in the field to obtain professional certification.

As one can see from Figure 2, 60 % of respondents (51 business participants) indicate the need for professional development based on in-house training.

Fig. 2. Types of advanced training for cybersecurity professionals

Figure 3 contains information on the ranking of countries with the largest number of certified cybersecurity professionals. The UK occupies the leading position, which proves high-quality certification and advanced training for cybersecurity professionals.

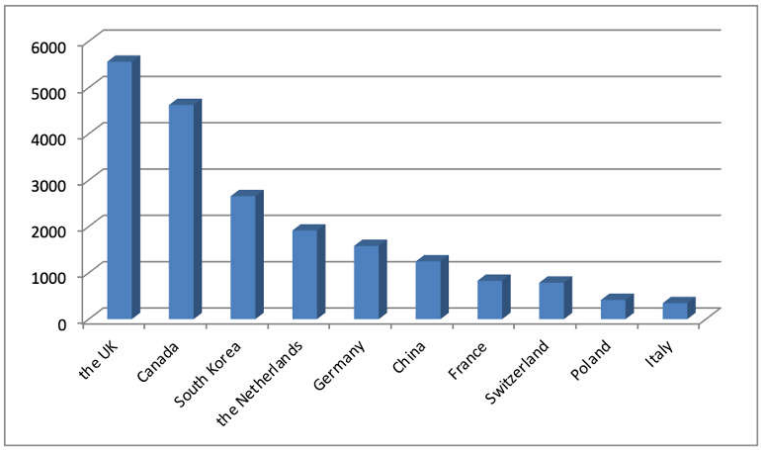

Fig. 3. The number of certified cybersecurity professionals in the world

The article funds that employers prefer certified professionals accredited by organizations such as CISSP, CISM, ISO27001LA, CLAS and others (see Figure 3).

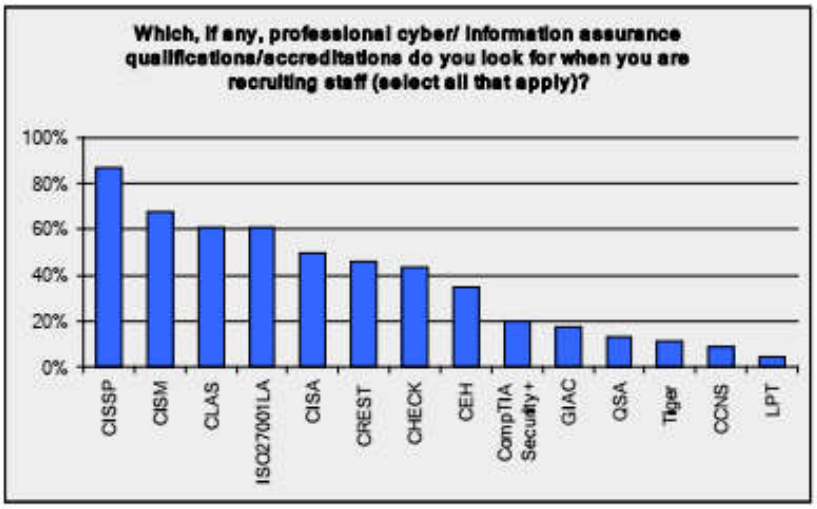

Fig. 4. The survey of employers on the certification of cybersecurity professionals in international organizations

Source: AMP International. (2020). *Cybersecurity*. Retrieved from https://apmg-cyber.com/products/ccp-cesg-certified-professional

CONCLUSIONS

Therefore, certification and advanced training of cybersecurity professionals in the UK is provided at the level of universities, international organizations. Besides, they take various forms (mainly online learning) on a paid basis, differ in the duration of the study and the content of courses. The following structures and companies are considered as most prestigious for employment (internship): "Accenture", "Canary Wharf", "Indonesian Ministry of Finance", "JP Morgan", "IBM", "Ministry of Defence", "Royal Mail", "Singapore Police", "CISCO", "Facebook" and many others. Importantly, they put forward significant demands on the certification of professionals.

The recognition of cybersecurity professionals' qualifications lies in two forms (state and certified). Certification takes place in the Academic Centres of Excellence in Cyber Security Research, the National Cyber Security Centre, as well as in public and private companies and international organizations. They create opportunities for obtaining the status of a Master in Cyber Security, a certified cybersecurity engineer, a certified IT support professional.

Further research should aim to determine the characteristics of professional certification and advanced training of cybersecurity professionals in the EU countries.

REFERENCES

1. AMP International. (2020). *Cybersecurity*. Retrieved from https://apmg-cyber.com/products/ccp-cesg-certified-professional

2. Cabinet Office. (2011). *The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world.* Retrieved from https://www.gov.uk/government/news/

protecting-and-promoting-the-uk-in-a-digital-world--3#:~:text=The%20Cyber%20Security%/20Strategy%20sets,trusted%20and%20resilient%20digital%20environment.&text=It%20heralds%20a%20new%20era,the%20world%20to%20do%20business.

3. *Chartered Institute of Information Security*. (2020). Retrieved from https://www.iisp.org/

4. Council of Europe. (1997). *The Convention on the Recognition of Qualifications concerning Higher Education in the European Region*. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/165.

5. ISO. (2012). *Conformity assessment – General requirements for bodies operating certification of persons.* Retrieved from https://www.iso.org/standard/52993.html.

6. National Cyber Security Centre. (2020). *CIISec, CREST and RHUL Consortium (CCP)*. Retrieved from https://www.ncsc.gov.uk/evaluation-partner/ciisec-crest-and-rhul-consortium-ccp

7. New Horizons. (2019). *The Best Cybersecurity Certifications to Boost Your Career in 2019.* Retrieved from *https://www.newhorizons.com/article/the-best-cybersecurity-certifications-to-boost-your-career-in-2018*

8. *SFIA*. (2020). Retrieved from https://sfia-online.org/en.

9. *The Chartered Institute for IT Professionals*. (2020). Retrieved from https://www.bcs.org/.

10. The National Cyber Security Center. (2018). *Certified professional scheme*. Retrieved from https://www.ncsc.gov.uk/information/about-certified-professional-scheme.