КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.129141
УДК 006.02:004.056

Tetiana M. Muzhanova
Ph.D. in Public Administration, Associate Professor, Associate Professor of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Yuriy M. Yakymenko
Ph.D. in Military Science, Associate Professor, Associate Professor of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Mykhailo M. Zaporozhchenko
Assistant of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

Vitalii M. Tyshchenko
Assistant of Information Security and Cyber Security Department
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0003-3849-6243
tvs5vetal@gmail.com

INTERNATIONAL VENDOR-NEUTRAL CERTIFICATION FOR INFORMATION SECURITY PROFESSIONALS

Abstract. When looking for qualified specialists in the field of IT and information security employers give preferences to candidates with professional certificates from reliable and worldwide recognized organisations. Attracting certified professionals allows the company to make the most efficient use of its staff and thereby increase its competitiveness. For qualified specialist, the certificate is a guarantee of his competence and the basis of confidence in a successful professional career.

Today, the market of IT and information security professional certification offers both certification programs from well-known software or hardware manufacturers, as well as vendor-neutral certifications, developed by expert organizations in this field and not related to the products of individual manufacturers.

Vendor-neutral certification programs provide a comprehensive approach to information security and ensure that certified specialists acquire understanding of technical and managerial aspects of information protection, as well as possess a wide range of diverse knowledge and practical skills.

The article researches the most popular and demanded on the market certification courses in information security from $(ISC)^2$, ISACA, EC-Council and CompTIA.

The authors found that reviewed certifications have the following common features: short training period of the certification programs, usually 5-7 days; joining both basic and specialized components within the courses; the use of well-known and mostly open hardware and software during training; combining various forms and methods of training: face-to-face and distance learning with an instructor, self-study, online tests and special learning platforms; conducting a comprehensive exam with the issuance of a certificate; three-year validity period of the certificate which must be confirmed through participation in scientific and practical activities in the specialty.

The study of international certification for information security specialists in Ukraine showed that there are several companies-authorized providers of certification services: ISSP Training Center, Fast Lane Group, Kyiv Chapter of ISACA, PwC Ukraine, which certify information security professionals through vendor-neutral courses, as well as certification programs of software and hardware developers.

Key words: International Vendor-Neutral Certification for Information Security Professionals; Professional Certification Programs in Information Security by $(ISC)^2$, ISACA, EC-Council, CompTIA; Certification for Information Security Professionals in Ukraine.

INTRODUCTION

One of the indicators of the maturity of the economy sector and the related labor market is the presence of professional organizations (often independent) that develop quality standards and conduct appropriate certification. Already today, employers in the field of IT and information security, when choosing employees, prefer candidates who have certificates from international expert organizations and manufacturers of software and hardware. It is likely that in the near future, certification will be as necessary for employment as a diploma of higher education.

Attracting certified professionals allows the company to get the most out of its staff and thus increase its competitiveness. For the most qualified specialist, the certificate is a guarantee of his competence and the basis of confidence in a successful professional career.

Various certifications are presented in the IT and information security market. The first category consists of certification programs from well-known manufacturers of software or hardware products, complex software and hardware solutions. The second includes the so-called vendor-neutral certifications, developed by expert organizations in this field and not related to the products of individual manufacturers.

Vendor-neutral certification programs aim to train professionals who can optimally organize and maintain comprehensive information security of the organization by combining different methods and technologies. Such certifications provide a comprehensive approach to information security: specialists need knowledge of technical and managerial aspects of information protection, as well as possession of a wide range of diverse knowledge and practical skills. Higher certifications of this type put forward a number of additional conditions to applicants, including the presence of several years of experience in the specialty and continuous improvement of their own skills to confirm the certificate.

RESEARCH OUTCOMES

Review of popular rankings of professional certifications in IT and information security [1, 2] showed that the most famous and demanded on the market are certificates provided by such international expert organizations as International Information Systems Security Certification Consortium $(ISC)^2$, Information System Audit and Control Association (ISACA), International Council of E-Commerce Consultants (EC-Council), Computing Technology Industry Association (CompTIA).

Certificates from $(ISC)^2$. According to experts, the International Information Systems Security Certification Consortium $(ISC)^2$ holds the lead in the implementation of Information Security certification programs.

$(ISC)^2$ is an international non-profit organization for testing and certification of information security professionals, which was established in 1989 in the United States and over

ISSN 2663 - 4023

the years has certified hundreds of thousands of security professionals from more than 85 countries [3]. Recently $(ISC)^2$ was named "the world's largest IT security organization".

CISSP. The most well-known certification program $(ISC)^2$ is the Certified Information Systems Security Professional (CISSP), which is considered the "gold standard" among certifications for high-level professionals. The first exam for CISSP, which is one of the highest information security certifications, was held in 1994.

The audience for this certification consists of representatives of middle and senior management in the field of information security - Security Architect, Chief Information Security Officer (CISO), Chief Security Officer (CSO), Director of Security, Vice President on security issues.

The requirements for applicants for CISSP status are quite strict: everyone must have at least 5 years of proven experience in the field of information security in two or more of the 8 parts of the program. This approach is standard for all known certifications and allows $(ISC)^2$ to weed out newcomers.

The updated CISSP certification program from May 1, 2021 contains 8 parts - domains, which are aimed at studying purely technical aspects of information security, including asset security and risk management, communications and network security, security architecture and engineering, identity and access management, security assessment and testing, security operations and software development security [4].

A 5-day training program has been developed to prepare for the CISSP exam. $(ISC)^2$ offers a variety of learning options: self-study, online courses or instructor-led courses in the classroom. Trainings, seminars, courseware and self-study aids can be obtained directly from $(ISC)^2$ or from one of its many official training providers. The same scheme is used for training in other programs $(ISC)^2$.

The exam is taken on a computer only in the examination classes of organizations accredited by $(ISC)^2$ and includes a large database of questions, which are updated annually to meet the current level of IT development, international law and information security standards. Detailed information on the CISSP and other ISC^2 exams is presented in Table 1.

Table 1.

Detailed information on the $(ISC)^2$ certification exams

	CISSP	SSCP	CCSP	CSSLP	HCISPP
Exam cost, USD	749	249	599		
Exam duration	6 hours	3 hours			
Number of domains	8	7	6	8	7
Number of questions	250	125			
Passing score	700 from 1000				
Exam language	English, French, German, Spanish, Portuguese, Japanese, Chinese, Korean	English, Portuguese, Japanese	English	English	English
Number of certified persons on 01.01.2022 [5]	152 632, 55 of them from Ukraine	6,881, 12 of them from Ukraine	10,898, 5 of them from Ukraine	3008, 2 of them from Ukraine	1419

After passing the exam, the specialist receives a certificate that is valid for 3 years. In addition to passing the exam, the CISSP candidate must sign the Consortium Code of Ethics $(ISC)^2$, which sets out the requirements for the holder of a prestigious certificate.

Due to the fact that the information security content and technologies are constantly changing and improving, the CISSP certificate is not lifelong and requires its owner to continuously work on updating their professional knowledge. To confirm this activity, each certificate owner periodically reports to the $(ISC)^2$ about the number of hours of Continuing Professional Education (CPE), gained in the process of participating in special educational programs. Thus, within 3 years, the certificate holder must obtain 120 CPE by writing profile articles, participating in conferences, seminars, trainings, etc.

This practice is mandatory for all Consortium $(ISC)^2$ certifications discussed below and certification programs from other vendor-independent providers.

It is important to note that CISSP holders can obtain additional certificates in the following three specializations in the field of information systems security:

1. CISSP-ISSAP - Information Systems Security Architecture Professional.
2. CISSP-ISSEP - Information Systems Security Engineering Professional.
3. CISSP-ISSMP - Information Systems Security Management Professional.

These CISSP specializations have lower requirements for the applicant: at least 2 years of practice; study 5-6 domains instead of 8; half the cost of the exam and the number of questions [4].

In addition to CISSP certification, the Consortium (ISC) offers other certification programs in the field of information security.

SSCP. The SSCP (Systems Security Certified Practitioner) certification course was developed by the Consortium $(ISC)^2$ for mid-level professionals who do not have sufficient experience to take the CISSP exam yet or are preparing for it, as well as for those who do not aspire to leadership positions and therefore do not need a higher status from $(ISC)^2$.

In general, SSCP certification is similar to CISSP except for minor differences, reflecting the lower requirements for the certificate holder: at least 1 year of professional experience; study 7 domains instead of 8; answer 125 questions instead of 250. The duration of the exam is twice less: 3 hours instead of 6.

The updated SSCP exam, which was unveiled in August and took effect in November 2021, includes the following 7 technical domains: Security Operations and Administration; Access Controls; Risk Identification, Monitoring and Analysis; Incident Response and Recovery; Cryptography; Network and Communications Security; Systems and Application Security.

CCSP. A relatively new qualification of the $(ISC)^2$ is the Certified Cloud Security Professional (CCSP). The CCSP certificate demonstrates that the specialist has advanced technical skills and knowledge for the design, management and protection of data, programs and infrastructure in the cloud, the use of best practices, policies and procedures established by information security experts of $(ISC)^2$.

CCSP certification is one of the few vendor-independent courses on cloud security and requires the candidate to have 5 years of experience in information security.

CCSP exam questions are divided into 6 domains, which contain purely technical topics on cloud concepts, architecture and design, cloud data security, cloud platform, infrastructure and applications, cloud security operations, as well as legal issues, risk management and compliance requirements.

CSSLP. Certified Secure Software Lifecycle Professional (CSSLP) certification confirms that the applicant has the basic knowledge and skills in application security, including

those required for authentication, authorization, and auditing in the software lifecycle, using best practices, policies and procedures established by the $(ISC)^2$ security experts. CSSLP certifies professionals who implement security methods and processes during software development.

Applicants are required to have a minimum of 4 years of software lifecycle experience to obtain this qualification status.

CSSLP certification from September 2020 includes 8 domains covering the following aspects of the secure software lifecycle: Concepts and Requirements, Architecture and Design, Implementation, Testing, Deployment, Operation, Maintenance, Supply Chain and Lifecycle Management.

HCISPP. HealthCare Information Security and Privacy Practitioner (HCISPP) is the only certification that combines security skills with best practices and methods of privacy ensuring. Applicants for the certificate must demonstrate knowledge and ability to implement, manage and evaluate control and privacy tools to protect the information of healthcare organizations, use policies and procedures established by information security experts of $(ISC)^2$.

As the HCISPP certificate is not intended for beginners, the applicant must have at least 2 years of professional experience and be competent in one or more of the 7 domains of the course.

The HCISPP certification program was updated in November 2019 and consists of 7 domains that reflect the specifics of information security in the healthcare industry including Information Governance and IT in Healthcare, Regulatory and Standards Environment, Privacy and Security, Risk Management and Risk Assessment, Third-Party Risk Management [4].

Certificates from ISACA. A significant contribution to the development of professional certification in the information security field is made by the Information System Audit and Control Association (ISACA). It is an international organization uniting professionals in IT audit, IT consulting, IT risk management and information security. As of today, ISACA has more than 200 local chapters in more than 180 countries, including 45 in Europe and 2 in the post-Soviet space, including in Kyiv [6].

ISACA currently offers several certifications in the field of information security, the most famous of which are CISA and CISM.

CISA. The Certified Information Systems Auditor (CISA) is the core ISACA certification. Since 1978, this certification reflects best practices in the field of IT-audit and information security.

The CISA certification cource consists of 5 domains, which cover the following issues: Information Systems Auditing Process; Governance and Management of IT; Information Systems Acquisition, Development and Implementation; Information Systems Operations and Business Resilience; Protection of Information Assets.

The last update of the CISA training course took place in June 2019, and the next one is scheduled for 2024 [7].

To prepare for the exams, ISACA offers several options: self-study, obtaining an annual subscription to a database of questions, answers and explanations on the content of the course or online review course, a 5-day training with an instructor in class or online.

Detailed information on the CISA exam and the other ISACA certification exams discussed below are presented in Table 2.

CISM. Certified Information Security Manager (CISM) is one of the most well-known certificates in the field of information security. It was developed by ISACA in 2002 specifically for managers in this sphere.

Among the main requirements for the CISM status are: professional experience in the information security field for at least 5 years and 3 of them - in managament positions.

The target groups of this certification are the information security middle and senior management - Director of Information Security (CISO), Director of Security (CSO), Vice President of Security.

The managerial direction of training is evidenced by the content of the CISM program, which contains 4 domains: Information Security Governance; Information Security Risk Management; Information Security Program; Information Security Incident Management.

CGEIT. Certified in the Governance of Enterprise IT (CGEIT) qualification from ISACA confirms that applicants have the expertise and experience needed to support corporate IT management. The course is designed for professionals with extensive experience in enterprise IT management. It is recognized worldwide as one of the highest qualifications in the field of information security.

The CGEIT certificate is awarded to candidates who have at least 5 years of relevant work experience and have successfully passed the exam. The CGEIT qualification course confirms the knowledge and skills of applicants in 4 domains: Governance of Enterprise IT; IT Resources; Benefits Realization; Risk Optimization.

Table 2.

Detailed information on the ISACA certification exams

	CISA	CISM	CGEIT	CRISC	CDPSE
Exam cost, USD	760 575 – for ISACA members				
Exam duration	4 hours				3,5 hours
Number of domains	5	4			3
Number of questions	150				120
Passing score	450 from 800				
Exam language	English, French, German, Spanish, Italian, Turkish, Japanese, Chinese, Korean	English, Spanish, Japanese, Chinese	English, Chinese	English, Spanish, Chinese	English
Number of certified persons [7]	More than 151,000	More than 48,000	More than 8,000	More than 30,000	-

CRISC. Certified in Risk and Information Systems Control (CRISC) is awarded to IT-professionals with experience in identifying and assessing IT risks, developing and monitoring measures to prevent, mitigate and overcome them.

This qualification is awarded to candidates who have at least 3 years of relevant work experience and have successfully passed the exam. They must show appropriate knowledge in 4 domains, which cover in detail the principles of Governance; IT Risk Assessment, Risk Response and Reporting, Information Technology and Security.

CDPSE. Certified Data Privacy Solutions Engineer (CDPSE) is the first of its kind technical certification that assesses an IT professional's ability of creating projects to improve technology platforms and products to ensure the confidentiality of information. The implementation of such solutions provides benefits for the organization and its customers, promotes trust and improves the confidentiality of information, including personal data.

The certificate applicant is required to have at least 3 years of practical experience in the following areas, which reflect the content of the 3 domains of the CDPSE program: Privacy Governance; Privacy Architecture and Data Life Cycle [8].

This certification program was implemented in 2020. There are no data on the number of certified specialists.

In order to successfully complete the preparation process and obtain these certificates from ISACA, it is desirable for the applicant to become a member of the Association, which will save on the cost of the exam and materials for its preparation.

The validity of each of the considered certificates is 3 years. Certificate holders who are ISACA members also pay an annual maintenance fee of $ 45. Certified professionals who are not members of the organization pay $ 85.

Certified specialists must sign the Code of Professional Ethics of the Association, according to which they are obliged to maintain the appropriate level of knowledge and qualifications in the relevant field. During the 3 years of validity of the certificates, their holders must constantly improve their competencies and receive at least 120 Continuing Professional Education (CPE) credits for the entire period and at least 20 CPE annually to maintain their accreditations. CPE credits can be obtained through participation in scientific and practical activities in the specialty, writing articles and other specialized publications, teaching, passing the relevant certification exams and volunteering to achieve the goals of the ISACA [7].

Certificates from CompTIA. A well-known professional organization engaged in independent certification in the field of IT and information security is the Computing Technology Industry Association (CompTIA), USA.

Today CompTIA implements professional certification courses in the following 4 areas in the field of IT:

1. Core: CompTIA IT Fundamentals (ITF+); CompTIA A+ (IT for beginners); CompTIA Network+; CompTIA Security+;

2. Infrastructure: CompTIA Cloud+; CompTIA Linux+; CompTIA Server+;

3. Cybersecurity: CySA+ (Cybersecurity Analyst); CompTIA PenTest+ (Penetration Testing Specialist); CompTIA CASP+ (Advanced Security Practitioner);

4. Additional professional certificates: CompTIA Project+ (IT projects specialist); CompTIA CTT+ (IT Technical Trainer); CompTIA Cloud Essentials+, CompTIA Data+ (Data analytics for beginners). The last certification was lauched in February 2022.

CompTIA claims to offer the largest non-vendor accreditation program for technology workers. Association has provided more than 2.5 million certificates in areas such as cybersecurity, networking, cloud computing and technical support [9].

CompTIA Security+. One of the most famous and popular CompTIA certifications is the program dedicated to information security - Security+.

Security+ is an international certification that confirms that the applicant has the basic skills needed to perform basic IT security functions and provides a foundation for middle-level positions and careers in information security.

Security+ is being constantly updated in line with the latest IT security trends, covering critical technical skills in risk assessment and management, incident response, digital forensics, corporate network security, cloud, mobile and IoT, IT security implementation, and more.

To obtain Security+ status, the candidate must have 2 years of experience in IT administration with an emphasis on security.

CompTIA Security+ certification exam, according to the updated in November 2020 version SY0-601, includes 5 domains: Attacks, Threats and Vulnerabilities; Architecture and Design of corporate security environments; Implementation (identity management, access

control, cryptography, wireless security and end-to-end security); Operations and Incident Response; Governance, Risk and Compliance (PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA) [10].

CompTIA CySA+. CySA+ is the only certificate for mid-level security analysts who must have at least 4 years of experience in information security or related fields, as well as CompTIA (Network+, Security+) or equivalent knowledge.

The CySA+ applicants must not only actively capture, monitor, analyze, and respond to network traffic data, but also have knowledge and skills in software and application security, threat detection, incident response, and compliance with IT and information security regulations.

The CySA+ program was updated in April 2020 and now contains 5 domains that cover the following issues: Threat and Vulnerability Management; Software and Systems Security; Compliance and Assessment; Security Operations and Monitoring; Incident Response.

CompTIA offers its own comprehensive interactive e-learning solutions for independent preparation for certification exams: CertMaster Learn (theoretical preparation), CertMaster Labs (practical training) and CertMaster Practice (assessment of knowledge and exam readiness). Preparatory trainings are conducted in class or online.

In addition to the traditional multiple-choice questions, the CompTIA Security+ and CySA+ certification exams include tasks that test a candidate's ability to solve problems in a simulated environment, such as a firewall or operating system. Testing of CompTIA certificate applicants is carried out online or in authorized points of the Association.

Detailed information about the exam for obtaining these CompTIA certificates is presented in Table 3.

Table 3.

Detailed information on the CompTIA certification exams

	Security+	CySA+
Exam cost, USD	381	
Exam duration	90 min.	165 min.
Number of domains	5	
Number of questions	90	85
Passing score	750 from 900	
Exam language	English, Japanese, Vietnamese, Thai, Portuguese	English, Japanese

Information about number of Security+ and CySA+ certificates holders is not available.

As in the above certification programs from other developers, CompTIA certificates are valid for a period of 3 years, and their owners undertake to participate in the Continuing Education Program to renew the existing certification. For example, Security+ holders must recieve at least 50 continuing education units (CEU) within 3 years, after which the certificate is automatically renewed [9].

EC-Council certifications. The International Council of E-Commerce Consultants (EC-Council) is an American non-governmental organization founded in 2001 after the infamous 9/11 attacks to provide certification and training services in e-business and cyber security. The founders of the Council see their goal as mitigating and eliminating the cyberplague that threatens the world today. During its existence, EC-Council has certified more than 200,000 professionals from 87 countries [11].

The organization is the owner and developer of the world-famous Certified Ethical Hacker (CEH) program and more than 20 courses in 6 categories:

1. **Advanced:** Certified SOC Analyst (CSA), Certified Penetration Testing Professional (CPENT), Licensed Penetration Testing Professional (LPT) Master, Web Application Hacking and Security, Certified Blockchain Professional (CBP), Advanced Network Defence, Advanced Penetration Testing (APT);

2. **Core:** CEN, CEN (Master), Certified Network Defender (CND), Certified Network Defence Architect (CNDA);

3. Fundamentals: Certified Cybersecurity Technician (CCT), EC-Council Certified Security Specialist (ECSS), EC-Council Certified Encryption Specialist (ECES), Network Defence Essential (NDE), Ethical Haker Essentials (EHE), Digital Forensics Essential (DFE);

4. **Specialist**: Computer Hacking Forensic Investigator (CHFI); Certified Cloud Security Engineer (CCSE), Certified Threat Intelligence Analyst (CTIA), EC-Council Certified Incident Handler (ECIH), Web Application Hacking and Security, Certified Application Security Engineer (CASE Net), Certified Application Security Engineer (CASE Java), EC-Council Disaster Recover Professional (EDRP);

5. **Management**: Certified Chief Information Security Officer (CCISO);

6. **Security Awareness**: Certified Secure Computer User (CSCU) and also NDE, EHE, DFE.

CEH. CEH certification, accredited by the American National Standards Institute (ANSI), is mandatory for ethical hacking IT professionals and proves their competence in five phases of ethical hacking: Reconnaissance; Scanning; Gain Access; Maintain Access; Cover Tracks.

In 2020, the EC-Council presented an updated version of CEH - Certified Ethical Hacker Version 11. Today, the CEH course consists of 20 modules, which include issues related to the actual algorithm and hacking methods (Footprinting and Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis, Malware Threats, Sniffing, Social Engineering, Denial-of-Service, Session Hijacking, Evading IDS, Firewalls, and Honeypots, SQL Injection, Cloud Computing, Cryptography), and the specifics of hacking various objects, including systems, web servers and applications, databases, wireless networks and mobile platforms, IoT and OT [12].

To obtain the CEN certificate, the applicants must have at least 2 years of practical experience in the field of information security or undergo formal training from the EC-Council in an accredited training center or through the iClass e-platform. The preparatory course lasts 5 days.

Certified CEH specialists can improve their professional level by obtaining CEN (Practical) qualification. To do this, they must pass a test, which consists in solving 20 practical problems. This exam is not a simulation and takes place in a real corporate network of virtual machines and programs with solutions to detect vulnerabilities. Upon completion of the CEH and CEH (Practical) programs, the title of CEH (Master) is awarded.

Detailed information about the CEH certification exams is presented in Table 4.

Table 4.

Detailed information on the CEH certification exams

	CEH (Master)	
	CEH (ANSI)	CEH (practical)
Exam cost, USD	1199	550
Exam duration	4 hours	
Number of modules	20	
Number of questions/tasks	125	20
Passing score	*	70%
Exam form	Test, multi-choice	Practical tasks
Exam language	English	

* The passing score is determined on the basis of knowledge and skills required to demonstrate competence in the subject, and in accordance with the complexity of the questions asked to the candidate.

Information about number of CEH certificates holders is not available.

After obtaining the status of CEH or other EC-Council certificates, certified specialists are obliged to constantly improve their professional level in accordance with the requirements of the EC-Council Continuing Education (ECE) policy. Within a 3-year period, certificate holders must receive 120 ECE credits

Common features of international certification programs for information security professionals. Thus, the analysis of the main certification courses implemented by international expert organizations $(ISC)^2$, ISACA, CompTIA and EC-Council, allows us to highlight the following their characteristics:

- certification programs have a short training period, usually 5-7 days;
- courses contain both basic and specialized components;
- given the independence of these certification courses from individual manufacturers, training is aimed at studying the general concepts and principles of professional activity and is based on the use of well-known and mostly open hardware and software;
- the programs combine different forms and methods of training: face-to-face and distance learning with an instructor, self-study, the use of electronic and paper textbooks, videos, online tests and special learning platforms;
- a mandatory element is to conduct a complex exam with the issuance of a certificate. Computer-adapted testing (CAT) is widely used;
- the validity of the certificate is three years, which reflects the general trends of dynamic development of technologies in the field of information security;
- self-education and professional development is a permanent and mandatory element of the professional activity of a certified ethical hacking specialist.

Certification of information security specialists in Ukraine. A study of the Ukrainian market of international certification programs in the field of information security has shown that the most well-known and in demand are the CISSP qualification programs from $(ISC)^2$; CISA and CISM from ISACA and various certifications from CompTIA.

In Ukraine, information security professionals can train and obtain international certificates from other expert organizations, such as SANS, ITIL, as well as software and hardware developers (Cisco, Microsoft, Oracle, IBM).

Training in international certification programs from $(ISC)^2$, ISACA, CompTIA and EC-Council in Ukraine is carried out by the following companies - authorized service providers:

- ISSP Training Center (CISSP, CISA, 9 CompTIA certifications, including Security+ and CySA+, 8 EC-Council certifications, including SEN, CPENT, CND, ESIN). ISSP Training

Center also develops tailor-made courses in information security, having previously agreed with the client the tasks and expected learning outcomes [13];

- Fast Lane Group (CISSP, 6 EC-Council certifications, including CEH, CND, CTIA, CHFI, ECIH, CPENT, CompTIA Security+) [14];
- Kyiv Chapter of ISACA (CISM, CISA, CGEIT and CRISC) [15];
- Price Waterhouse Coopers (PwC) Ukraine (CISM, CISA) [16].

It should be noted that the offices of all these organizations are located in Kyiv. PwC Ukraine has branches in Lviv and Dnipro.

In general, the activities of organizations and training centers for certification of specialists in the field of information security are aimed at forming a "new class" of specialists who will acquire unique skills and ensure the competitiveness of their companies not only in domestic but also in international markets.

CONCLUSION

Analysis of the most famous vendor-neutral certification courses in information security by $(ISC)^2$, ISACA, CompTIA and EC-Council revealed such common features: short training period of the certification programs, usually 5-7 days; joining both basic and specialized components within the courses; using well-known and mostly open hardware and software during training; combining different forms and methods of training: face-to-face and distance learning with an instructor, self-study, online tests and special learning platforms; conducting a comprehensive exam with the issuance of a certificate; three-year validity of the certificate which must be confirmed by self-education and training.

Research results of the Ukrainian market of international certification in information security showed that there are several companies-authorized providers of certification services: ISSP Training Center, Fast Lane Group, Kyiv Chapter of ISACA, PwC Ukraine, which certify information security professionals as within vendor-independent courses ((ISC)2, ISACA, CompTIA and EU-Council), as well as through software and hardware developers certification programs (Cisco, Microsoft, Oracle, IBM and others).

REFERENCES

1 7 top security certifications you should have in 2022. https://resources.infosecinstitute.com/topic/7-top-security-certifications-you-should-have/
2 10 Popular Cybersecurity Certifications 2022. https://www.coursera.org/articles/popular-cybersecurity-certifications
3 About ISC².https://www.isc2.org/about. URL: ttp://www.isc2.org
4 (ISC)² certifications. https://www.isc2.org/Certifications
5 (ISC)² member counts. https://www.isc2.org/About/Member-Counts
6 Information Systems Audit and Control Association. http://www.isaca.org.ua/index.php/homepage/about
7 ISACA credentialing. https://www.isaca.org/credentialing/
8 ISACA Certification Exam Candidate Guide. (2019). *ISACA*. https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/exam%20candidate%20guides/exam-candidate-guide-continuous-testing
9 CompTIA Certifications. https://www.comptia.org/certifications
10 CompTIA Security+. https://www.comptia.org/certifications/security
11 EC-Council. About us. https://www.eccouncil.org/about/
12 CEH V11. Program Broshure. (2020). *EC-Council.* https://www.eccouncil.org/wp-content/uploads/2020/09/CEHv11-Brochure.pdf
13 ISSP Training Center. Наші тренінги. https://www.issp.training/courses
14 Професійна підготовка і IT кваліфікація. https://www.flane.com.ua/ua/training
15 Професійна сертифікація від ISACA. http://www.isaca.org.ua/index.php/certification
16 PwC в Україні. Сертифікації. https://www.pwc.com/ua/uk/services/corporate_trainings/certification.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Мужанова Тетяна Михайлівна
к.держ. упр., доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Якименко Юрій Михайлович
к.військ.н. доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0002-6848-852X
yakum14@ukr.net

Запорожченко Михайло Михайлович
Асистент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

Тищенко Віталій Сергійович
Асистент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0003-3849-6243
tvs5vetal@gmail.com

МІЖНАРОДНІ НЕЗАЛЕЖНІ ВІД ВИРОБНИКІВ СЕРТИФІКАЦІЙНІ ПРОГРАМИ ДЛЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Шукаючи кваліфікованих спеціалістів у сфері ІТ та інформаційної безпеки роботодавці віддають перевагу кандидатам з професійними сертифікатами від надійних та всесвітньо визнаних організацій. Залучення сертифікованих фахівців дозволяє компанії максимально ефективно використовувати свій персонал і тим самим підвищувати конкурентоспроможність бізнесу. Для кваліфікованого спеціаліста сертифікат є запорукою його компетентності та основою впевненості в успішній професійній кар'єрі.

Сьогодні ринок професійної сертифікації з ІТ та інформаційної безпеки пропонує як програми сертифікації від відомих виробників програмного або апаратного забезпечення, так і незалежні сертифікати, розроблені експертними організаціями в цій галузі і не пов'язані з продукцією окремих виробників.

Незалежні сертифікації забезпечують комплексний підхід до інформаційної безпеки та гарантують, що сертифіковані спеціалісти є компетентними з технічних та управлінських аспектів захисту інформації, а також володіють широким спектром різноманітних знань і практичних навичок.

У статті досліджено найбільш популярні й затребувані на ринку професійні сертифікаційні курси з інформаційної безпеки від $(ISC)^2$, ISACA, EC-Council та CompTIA. Встановлено, що розглянуті сертифікації мають такі спільні риси: короткий термін навчання за програмами сертифікації, зазвичай 5-7 днів; поєднання в межах курсів як базових, так і спеціалізованих компонентів; використання під час навчання переважно відкритих апаратних і програмних засобів; поєднання різноманітних форм і методів навчання: очне або дистанційне навчання з інструктором, самостійне навчання, онлайн-тести та використання спеціальних навчальних платформ; проведення комплексного іспиту з подальшою видачею сертифіката; трирічний термін дії сертифіката, який необхідно підтверджувати шляхом участі в наукових та практичних заходах за спеціальністю.

Дослідження ринку міжнародної сертифікації фахівців з інформаційної безпеки в Україні показало, що існує кілька компаній - акредитованих постачальників послуг професійної сертифікації: Треніговий центр ISSP, група компаній Fast Lane, Київське відділення ISACA, компанія PwC в Україні, які сертифікують фахівців із інформаційної безпеки шляхом проведення незалежних від виробників курсів, а також сертифікаційних програм від розробників програмного та апаратного забезпечення.

Ключові слова: міжнародні незалежні від виробників сертифікаційні програми для фахівців з інформаційної безпеки; програми професійної сертифікації з інформаційної безпеки від (ISC)^2, ISACA, EC-Council, CompTIA; сертифікація спеціалістів із інформаційної безпеки в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 7 top security certifications you should have in 2022. https://resources.infosecinstitute.com/topic/7-top-security-certifications-you-should-have/
2 10 Popular Cybersecurity Certifications 2022. https://www.coursera.org/articles/popular-cybersecurity-certifications
3 About ISC^2. https://www.isc2.org/about. URL: ttp://www.isc2.org
4 (ISC)² certifications. https://www.isc2.org/Certifications
5 (ISC)² member counts. https://www.isc2.org/About/Member-Counts
6 Information Systems Audit and Control Association. http://www.isaca.org.ua/index.php/homepage/about
7 ISACA credentialing. https://www.isaca.org/credentialing/
8 ISACA Certification Exam Candidate Guide. (2019). *ISACA.* https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/exam%20candidate%20guides/exam-candidate-guide-continuous-testing
9 CompTIA Certifications. https://www.comptia.org/certifications
10 CompTIA Security+. https://www.comptia.org/certifications/security
11 EC-Council. About us. https://www.eccouncil.org/about/
12 CEH V11. Program Broshure. (2020). *EC-Council.* https://www.eccouncil.org/wp-content/uploads/2020/09/CEHv11-Brochure.pdf
13 ISSP Training Center. Наші тренінги. https://www.issp.training/courses
14 Професійна підготовка і IT кваліфікація. https://www.flane.com.ua/ua/training
15 Професійна сертифікація від ISACA. http://www.isaca.org.ua/index.php/certification
16 PwC в Україні. Сертифікації. https://www.pwc.com/ua/uk/services/corporate_trainings/certification.html