Syllabus

Attestation (Unified State Qualification Exam (USQE))

Specialty
125 Cybersecurity and information protection

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Cybersecurity

Department
Cybersecurity (328)

Level of education
Bachelor's level

Course type
Special (professional), Mandatory

Semester
8

Language of instruction
English

Developers

Serhii YEVSEIEV

serhii.yevseiev@khpi.edu.ua
Doctor of technical sciences, professor, head of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 350, including 42 utility model patents, 17 monographs, of which 9 are collective monographs, 31 textbooks, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 163 articles in foreign publications and specialized publications of Ukraine, with 61 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "Introduction to networks", "Security of banking systems", "Hybrid warfare and national security", "Audit and monitoring of corporate networks", "Blockchain: basics and application examples", "Fundamentals of smart contracts", "Basics of cyber security" for undergraduate and graduate students, Section "Methods and technologies of information security monitoring and auditing", "Methods of building post-quantum cryptosystems", "Latest technologies for ensuring cyber security based on blockchain technology" for postgraduate students.

More about the lecturer on the department's website

General information

Summary

The summary states that attestation is the final step in the training of students of the appropriate level of higher education in the educational and professional program. The unified state qualification exam provides for the assessment of learning outcomes, determined by the Standard of Higher Education and the educational and professional program in the specialty "Cybersecurity and Information Protection".

Objectives of the educational component

The purpose of attestation is: to expand and consolidate the competencies and learning outcomes acquired by the student during the study within the relevant educational and professional (educational and scientific) program; to assess the level of formation of graduates' competencies prescribed by the relevant level of the national qualifications framework and educational and professional (educational and scientific) program of professional training in accordance with the requirements of the higher education standard.

Format of the educational component

Self-study, consultations. Final control: attestation in the form of a unified state qualification exam.

Competencies

IC The ability to solve complex specialized tasks and practical problems in the field of ensuring information security and/or cyber security, characterized by complexity and incomplete determination of conditions.
GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-3. Ability to abstract thinking, analysis and synthesis.
GC-4. Ability to identify, state and solve problems in a professional manner.
GC-5. Ability to search, process and analyze information.
GC-6. The ability to realize own rights and responsibilities as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.
GC-7. The ability to preserve and multiply moral, cultural, scientific values and achievements of society based on an understanding of the history and patterns of development of the domain, its place in the general system of knowledge about nature and society and in the development of society, technologies, to use various types and forms of motor activity for active recreation and leading a healthy lifestyle.
PC-1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems.
PC-4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.
PC-5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy.
PC-6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and refusal of various classes and origins.
PC-7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.).
PC-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-9. Ability to perform professional activities based on the implemented information and/or cyber security management system.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC-11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
PC-12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security

Learning outcomes

LO-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LO-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LO-3. Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity.
LO-4. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made.
LO-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LO-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LO-7. Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security.
LO-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LO-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LO-10. Perform analysis and decomposition of information and telecommunication systems.
LO-11. Perform analysis of connections between information processes on remote computer systems.
LO-12. Develop threat and intruder models.
LO-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by hardware and software tools and evaluate the effectiveness of the quality of the decisions made.
LO-15. Use modern hardware and software of information and communication technologies.
LO-16. Implement complex information security systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. Ensure the processes of security and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of security of electronic information resources with a reflection of relationships and information flows, processes for internal and remote components.
LO-18. Use software and software-hardware complexes for the security of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LO-21. Solve tasks of provision and support (including: review, testing, accountability) of the access control system according to the stated security policy in information and telecommunication (automated) systems.
LO-22. Solve the management procedures of identification, authentication, authorization of processes and users in information and telecommunication systems according to the established policy of information and/or cyber security.
LO-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LO-24. Solve the problems of managing access to information resources and processes in information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based).
LO-25. Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and telecommunication (automated) systems using event registration logs, their analysis and stated protection procedures.

LO-26. Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model of interaction of open systems.
LO-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security.
LO-29. Evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means under the conditions of realization of threats of various classes.
LO-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
LO-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LO-32. Solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the stated security policy.
LO-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LO-34. Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization.
LO-35. Solve the tasks of providing and supporting complex information security systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the stated policy of information and/or cyber security.
LO-36. Detect dangerous signals of technical means.
LO-37. Measure the parameters of dangerous and interfering signals during the instrumental control of information security processes and determine the effectiveness of information security against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information security system.
LO-38. Interpret the results of special measurements using technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information security system.
LO-39. Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents.
LO–40. Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information security system.
LO-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LO-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LO-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LO-44. Solve the problems of ensuring the continuity of the organization's business processes on the basis of risk management theory and the stated information security management system, in accordance with national and international requirements and standards.
LO-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LO-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LO-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LO-48. Implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.

LO-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.
LO-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LO-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LO-52. Use tools for monitoring processes in information and telecommunication systems.
LO-53. Solve problems of software code analysis for the presence of possible threats.
LO-54. Be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine.

Student workload

The total volume is 180 hours (6 ECTS credits): self-study - 180 hours.

Prerequisites for the educational component

For successful attestation, it is necessary to acquire competencies and program results from all previous educational components of the program and successfully complete practical training.

Requirements and features of the educational component

USQE contains tasks with a concise and understandable description, covering the areas of the legislative and regulatory framework for information and/or cyber security, information and/or cyber security management, cryptographic and technical information protection, security of information and communication systems, complex information protection systems.
USQE is conducted according to the following principles: academic integrity; objectivity; transparency and publicity; intolerance to corruption and corruption-related acts; integration into the international educational and scientific space; the unity of the method of evaluation of results.

Program of the educational component

Attestation is the assessment of the compliance of a particular level of education and the scope of knowledge, skills, and competencies acquired by students with the requirements of higher education standards.

The unified state qualification exam is conducted in the form of external independent assessment in accordance with the USQE program, using various types of tasks.
The tasks of the qualification exam are developed in accordance with the program of USQE.
The USQE program consists of sections on the legislative and regulatory framework, state and international requirements, practices and standards in the field of information and/or cyber security; information technologies in information and/or cyber security; security of information and communication systems; complex information protection systems; management of information and/or cyber security; cryptographic protection of information; technical information protection.

Materials and recommended reading

Basic materials and provisions:

1. On higher education: Law of Ukraine (Vidomosti Verkhovna Rada (VVR), 2014, No. 37-38, Article 2004). URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text
2. On education: Law of Ukraine (Vidomosti Verkhovna Rada (VVR), 2017, No. 38-39, Article 380). URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text
3. Standard of higher education in the specialty 125 Cybersecurity and information protection for the first (bachelor) level of higher education dated October 4, 2018 No. 1074, taking into account changes in the Standard of higher education in the specialty 125 Cybersecurity and information protection (order of the Ministry of Education and Science of Ukraine from 13.01.2022 No. 26) URL: https://mon.gov.ua/static-

objects/mon/sites/1/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf
4. Program of the unified state qualification exam in specialty 125 Cybersecurity at the first (bachelor) level of higher education (order of the Ministry of Education and Science of Ukraine dated November 4, 2022 No. 980) URL: https://kb.khmnu.edu.ua/wp-content/uploads/sites/6/63861d8f5ff01844854871.pdf
5. Resolution on the attestation of the holders of the degree of professional preliminary education and degrees of higher education at the first (bachelor's) and second (master's) levels in the form of a single state qualification exam. URL: https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text
6. Regulations on the organization of the educational process at the National Technical University "Kharkiv Polytechnic Institute" (third edition) (Protocol of the Academic Council No. 6 dated 07.05.2024) URL: https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2024/09/Polozhennya_pro_organizatsiyu_osvitnogo_2024_final_pravka_3.pdf

Additional references:

1. Yevseyev S.P. Cyber security: modern protection technologies. / Evseev S.P., Ostapov S.E., Korol O.G. // Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678. - Access mode: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Information protection technologies./ S.E. Ostapov, S.P. Yevseev, O.G. King. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.
3. Bonaventure O. Computer Networking: Principles, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p.
https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf.
4. Yevseev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
5. Security of information and communication systems. K.: VNV Publishing Group, 2009. – 608 p.
https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf
6. Bogush V. M., Yudin O. K. Information security of the state. - K.: "MK-Press", 2005. - 432p.
7. Terminological reference book on technical information protection / Kozhenevskyi S.R., Kuznetsov G.V., Khoroshko V.O., Chirkov D.V. / Under the editorship Prof. V.O. Good girl - K.: DUIKT, 2007.- 365 p.
8. Bobalo Yu.Ya., Horbatii I.V. (ed.) Information security. Study guide. - Lviv: Publishing House of Lviv Polytechnic, 2019. - 580 p. - ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
9. Information security of the state: education. manual for students special 6.170103 Management of Information Security, 125 Cyber Security / V.I. Guryev, D.B. Mehed, Yu.M. Tkach, I.V. Firsova. – Nizhin: FOP Lukyanenko V.V. TPK "Orkhideya", 2018. - 166 p. URL:
https://ir.stu.cn.ua//bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
10. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
12. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

13. On information protection in information and telecommunication systems: Law of Ukraine dated 07.05.1994 No. 80/94-VR. Update date: 12/31/2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
14. On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. Update date: 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
15. Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated May 6, 2015 No. 287/2015. Date of update: 16.09.2020. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text
16. On national security: Law of Ukraine dated June 21, 2018 No. 2469-VIII. Date of update: 03/31/2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
17. Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine" No. 96/2016. Update date: 08/28/2021. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
18. Regulation on technical protection of information in Ukraine, approved by the Decree of the President of Ukraine dated 09/27/99 No. 1229. Date of update: 05/04/2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text
19. DSTU 3396 0-96 Information protection. Technical protection of information. Basic provisions. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
20. DSTU 3396 1-96 Information protection. Technical protection of information. The order of work. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
21. ND TZI 1.4-001-2000 Standard provision on the information protection service in automated systems, order of the DSTSZI of the SBU dated 04.12.2000 No. 53 (Amendment No. 1 order of the State Special Communications Administration dated 28.12.2012 No. 806). URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf
22. ND TZI 2.5-004-99 Criteria for evaluating the security of information in computer systems against unauthorized access, order of the DSTSZI of the SBU dated 04.28.99 No. 22 (Amendment No. 1 order dated 12.28.2012 No. 806). URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
23. ND TZI 2.5-005-99 Classification of automated systems and standard functional profiles of protection of processing information against unauthorized access, order of the DSTSZI of the SBU dated 04.28.99 No. 22 (Amendment No. 1 order dated 10.15.2008 No. 172). URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf
24. ND TZI 3.6-003-16 Protection of information at the objects of information activity. Creation of a complex of technical protection of information. Basic provisions.
25. ND TZI 3.7-003-2023 The procedure for carrying out work on the creation of a comprehensive information protection system in the information and communication system (Order of the Administration dated 10/28/2023 No. 924). URL: https://www.cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-vnesennya-zmin-do-normativnogo-dokumenta-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi-3- 7-003-2005-vid-28-zhovtnya-2023-roku-924
26. ND TZI 1.6-004-2013 Protection of information at objects of information activity. Provisions on the categorization of objects where information with limited access, constituting a state secret, circulates. URL: https://zakononline.com.ua/documents/show/83554__83554
27. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e. https://www.coursehero.com/file/55121963/handbook-all-engpdf/
28. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://www.iso.org/ru/contents/data/standard/08/28/82875.html
29. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html
30. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL: https://www.iso.org/ru/contents/data/standard/08/05/80585.html

Assessment and grading

Criteria for assessment of student performance and the final score structure

The criteria for assessment the results of the qualification exam in the specialty "Cybersecurity and information protection" are approved by the responsible state institutions (Ministry of Education, State Special Communications Administration, Ministry of Defense).
Completion of all exam tasks from the unified state qualification exam is mandatory. The final grade of the comprehensive exam is defined as the average of the positive grades for each type of exam tasks.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic ethics and integrity

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed, and if it is impossible to resolve the conflict, the issue should be brought to the attention of the Institute's management. Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website:
http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by	Date, signature 28.08.2024	Head of the department Serhii YEVSEIEV
	Date, signature 28.08.2024	Guarantor of the educational program Serhii YEVSEIEV