Syllabus
Practice Program

Technological practice

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

Type of the educational component
Practical training. 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

Alla HAVRYLOVA

alla.havrylova@khpi.edu.ua
PhD, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 30, including 2 utility model patents, 3 monographs, of which 1 is in a peer-reviewed edition included in the Scopus database, 1 is in a foreign scientific publication, 2 is in a specialized publication of Ukraine; 14 articles, of which 7 scientific articles are in Ukrainian scientific publications, 4 scientific articles are in peer-reviewed publications included in the Scopus database, 3 articles are in foreign scientific publications.

Lecturer on disciplines: "Introduction to the specialty. Introductory practice", "Organizational provision of information protection" for undergraduate students

More about the lecturer on the department's website

General information

Summary

When completing this type of practice, applicants develop qualification and professional competence based on the synthesis of theory and practice, and it manifests itself through the actualization of the individual's ability not only to solve professional tasks, but also to raise and solve professional problems.

Objectives and goals

Acquisition by students of professional skills and the ability to carry out independent research and professional work.

Format of activities

Independent work, self-study, individual assignment (report, practice diary), consultations. The final control is a test.

Competencies

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.
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.
LOR-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.

Duration of the practice

The duration of the practice is 4 weeks.

Prerequisites for the educational component

Disciplines of general and special training in 1-8 semesters of study according to the list of educational components.

Features of the educational component, teaching and learning methods, and technologies

Technological practice is carried out at enterprises (organizations, institutions) on the basis of concluded agreements with the regulation of the main issues of the organization of work of interns. Direct supervision of practice is carried out by the head of practice from the University (from among the teachers of the graduation department). At the beginning of practice, students of higher education must receive instruction on labor protection in the industry, familiarize themselves with the procedure for obtaining documentation and materials. Students of higher education during internships are obliged to:
- before the beginning of the internship, receive from the supervisor of the internship from the University referrals, methodological materials (methodical instructions, program, diary, individual assignment) and consultations on the preparation of the necessary documents;
- arrive at the practice base on time;
- visit the practice base daily;
- perform all tasks in full;
- study and observe the rules of labor protection, safety and industrial sanitation and internal regulations;
- be responsible for the work performed and its results;
- keep a practice diary;
- timely prepare the reporting documentation and make a credit from the practice.

The general form of practice reporting is the submission of a written report. The main document that reflects the current activities of the student of higher education, the stages of completing tasks, is a practice diary. This document is part of the report of the applicant of higher education. Keeping a diary is mandatory during the internship. The report together with other documents (practice diary; characteristics with an evaluation of the practice by the head of the practice at the enterprise) is submitted to the defense. The report includes information on the implementation of all sections of the practice program and individual assignment, as well as sections on occupational health and safety, conclusions and proposals, a list of used literature, etc. The report is prepared in accordance with the uniform requirements for the preparation of text documents. The student of higher education defends the internship report (with a differentiated assessment) in the commission, which includes the managers of the internship (if possible, from the internship bases), scientific and pedagogical workers who taught special disciplines. The composition of commissions is approved by the head of the department.

Topics of the individual assignment

The topic is determined taking into account the place of practice with the consent of the managers from the educational institution and the place of practice or the main directions of the individual task are presented.
Examples of individual task topics:
Topic 1. Development and implementation of a system of protection against malicious software.
Topic 1. Configuring firewalls.
Topic 1. Installation and configuration of the intrusion detection and prevention system (IDS/IPS).
Topic 1. VPN configuration for secure remote access.
Topic 2. Data encryption and implementation of cryptographic systems.
Topic 3. Development and implementation of the access control system (Access Control).
Topic 4. Network protection using VLAN and segmentation.
Topic 5. Development of a data backup and recovery system.
Topic 6. Network security monitoring using SIEM.
Topic 7. Analysis and improvement of web application security.
Topic 8. Implementation of multifactor authentication (MFA).
Topic 9. Integration of solutions for the protection of cloud services.
Topic 10. System penetration testing (Penetration Testing).
Topic 11. Development of the organization's cyber security policy.
Topic 12. Threat assessment and cyber risk management.
Topic 13. Protection of mobile devices in the corporate environment (BYOD).
Topic 14. Implementation of protection systems against DDoS attacks.
Topic 15. Security analysis of the Internet of Things (IoT).
Topic 16. Incident management and response to cyber incidents.
Topic 17. Development of secure communication channels (VPN, SSL/TLS).

Materials and recommended reading

References:

1. DSTU 8302:2015 Information and documentation. Bibliographic reference. General provisions and rules of compilation. – Kyiv: SE "UkrNDNC", 2016. – 17 p.
http://lib.pnu.edu.ua/files/dstu-8302-2015.pdf.
2. DSTU 3008-15 Information and documentation. Reports in the field of science and technology. Structure and design rules. – Kyiv: SE "UkrNDNC", 2016. – 31 p.
https://science.kname.edu.ua/images/dok/derzhstandart_3008_2015.pdf.
3. DSTU 1.5:2015 National standardization. Rules for the development, teaching and registration of regulatory documents. – Kyiv: SE "UkrNDNC", 2015. – 65 p.
https://udhtu.edu.ua/wp-content/uploads/2018/03/DSTY_1_5_2015.pdf.
4. Danilyan O. G. Dzoban O. P. Methodology of scientific research: a textbook - Kharkiv: Pravo, 2019. - 368 p.
https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf
5. Methodical instructions for conducting industrial practice [Electronic resource]: for students of the first (bachelor's) level of higher education for special. 125 "Cyber security and information protection" / editor: S. P. Yevseev, O. G. Korol, A. A. Gavrilova; National technical University "Kharkiv Polytechnic Institute". - Electron. text. data. – Kharkiv: NTU "KhPI", 2024. – 22 p. – URI:
https://repository.kpi.kharkov.ua/handle/KhPI-Press/81233.
6. STZVO-KhPI-3.01-2021 SSONP. Text documents in the field of educational process. General requirements for performance (with changes). URL: https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-3.01-2021-SSONP.-Tekstovi-dokumenti-u-sferi -navchalnogo-protsesu.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf.
7. 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.

Additional references:

8. Havrylova A., Khokhlachova Y., Tkachov A., Voropay N., Khvostenko V. Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal. 2023, Vol. 25, no. 1. R. 6-19.
https://jrnl.nau.edu.ua/index.php/ZI/article/view/17593
9. Yevseyev S., Havrylova A., Milevskyi S., Sinitsyn I. and others. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023, No. 3/9 (123). R. 33-48.
https://journals.uran.ua/eejet/article/view/281795/277627
10. Ethernet technology: laboratory workshop / M. O. Bilova, S. P. Yevseev, O. S. Zhuchenko, I. S. Ivanchenko, O. V. Shmatko. - Lviv: "New World - 2000", 2020. - 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
11. Yevseyev S.P. CYBER SECURITY: LABORATORY PRACTICUM ON THE FUNDAMENTALS OF CRYPTOGRAPHIC PROTECTION / S.P. Yevseev, O.V. Milov, O.G. Korol - Lviv: "New World-2000", 2020. - 241 p.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf
12. Yevseev S.P., Zhenyuk N.V., Okhrimenko M.Yu., Golovashich S.O., Kudiy D.A. E25 Digital circuitry and architecture of microprocessors: a study guide / Yevseev S.P., Zhenyuk N.V., Okhrimenko M.Yu. etc. - Kharkiv, - Lviv: Publishing House of PP "Noviy Svit - 2000", 2023. - 513 p.
https://drive.google.com/file/d/1fTWF7v4v-aaCL_oHMSHsyIJOrNlEu9v-/view
13. 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.
14.On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. Date of update: 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
15. Chmylenko F.O., Zhuk L.P. Guide to the study of the discipline "Methodology and organization of scientific research" - Dnipro: RVV DNU, 2014. - 48 p.
http://kist.ntu.edu.ua/textPhD/mond.pdf
16. Methodology and organization of scientific research. [text]: teaching manual / G.O. Birta, Yu.G. Burgu – Kyiv: Center for Educational Literature, 2014. – 142p.
https://shron1.chtyvo.org.ua/Burhu_Yurii/Metodolohiia_i_orhanizatsiia_naukovykh_doslidzhen.pdf

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
• implementation and design of the practice report (70%);
• the result of the assessment in the form of a test (30%).

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, including when visiting the practice site. Conflict situations should be openly discussed in academic groups with lecturers and supervisors, and if it is impossible to resolve the conflict, they 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