Syllabus

Course Program

Comprehensive training

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

Lecturers and course developers

Stanislav MILEVSKYI

Stanislav.Milevskyi@khpi.edu.ua

Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 100 scientific and educational and methodological works. Scientific Guarantor of the educational and scientific program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Fundamentals of Mathematical Modeling of Security Systems", "English in Academic Applications", "Modeling of Cyber-Physical Actions" for undergraduate and graduate students.

More about the lecturer on the department's website

Natalya VOROPAY

voropay.n@gmail.com

Candidate of Technical Sciences, associate professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The author of more than 30 scientific and educational works. Leading lecturer in the disciplines: "Programming technologies Part 1", "Decentralized systems", "Protection of critical infrastructure objects", "Antivirus protection of information", "Blockchain and smart technologies" in electronic document circulation".

More about the lecturer on the department's website

General information

Summary

The educational discipline "Comprehensive training" is a mandatory educational discipline. The discipline is aimed at students acquiring practical skills in identifying and countering modern threats in cyberspace.

Course objectives and goals

Formation of students' practical skills in identifying and countering modern threats in cyberspace on the basis of working out practical tasks.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - credit 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.
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 of the course is 120 hours (4 ECTS credits): lectures - 24 hours, laboratory classes - 36 hours, self-study - 60 hours.

Course prerequisites

Antivirus protection of information, Integrated information security systems.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. Implementation of the code.
Detection of injections such as SQL, NoSQL, OS, and LDAP injection that occur when untrusted data is sent to the interpreter as part of a command or query.
Topic 2. Incorrect authentication and session management.
Exposing application features related to authentication and session management that allow attackers to compromise passwords, keys, or rock tokens or exploit other implementation flaws to temporarily or permanently assume the identity of other users.
Topic 3. Cross-site scripting (XSS).
Detect web applications and APIs that are not properly secured. Criminals can steal or modify such weakly protected data to commit credit card fraud, identity theft, or other crimes.
Topic 4. Dangerous direct references to objects.
Analysis of old or poorly configured XML processors evaluate external object references in XML documents. External objects can be used to expose internal files using a file URI handler, internal file sharing, internal port scanning, remote code execution, and denial of service attacks.
Topic 5. Dangerous configuration.
Constraint analysis of what users are allowed to do is often not done properly. Attackers can use these flaws to access unauthorized functionality and/or data, such as accessing other users' accounts, viewing confidential files, changing other users' data, changing access rights, etc.
Topic 6. Leakage of sensitive data - assessment of security configuration.
This is usually the result of unsafe default configurations, incomplete or custom configurations, exposed cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries and applications be reliably configured, but they must be patched / upgraded in a timely manner.
Topic 7. Lack of access control to the functional level.
Identifying XSS flaws that occur whenever an application includes untrusted data in a new web page without proper validation or opening, or updates an existing web page with user-supplied data using a browser API that can generate HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser that can hijack user sessions, destroy websites, or redirect the user to malicious sites.

Topic 8. Forgery of cross-site requests (CSRF).
Evaluation of dangerous deserialization, which often leads to remote code execution. Even if deserialization deferrals do not result in remote code execution, they can be used to perform attacks including replay attacks, injection attacks, and privilege escalation attacks.
Topic 9. Using components with known vulnerabilities.
Analysis of components such as libraries, frameworks, and other software modules that run with the same privileges as the application. If a vulnerable component is used, such an attack can facilitate serious data loss or server hijacking. Applications and APIs that use components with known vulnerabilities can subvert defense applications and enable various attacks and impacts.
Topic 10. Unvalidated redirects.
Insufficient accounting and monitoring, combined with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain resilience, convert more systems, and tamper with, extract, or destroy data. Most breach investigations reveal breach detection times of more than 200 days, typically detected by external parties rather than internal processes or monitoring.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Implementation of the code.
Topic 2. Incorrect authentication and session management.
Topic 3. Cross-site scripting (XSS).
Topic 4. Dangerous direct references to objects.
Topic 5. Dangerous configuration.
Topic 6. Leakage of sensitive data - assessment of security configuration.
Topic 7. Lack of access control to the functional level.
Topic 8. Forgery of cross-site requests (CSRF).
Topic 9. Using components with known vulnerabilities.
Topic 10. Unvalidated redirects.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
Subjects are not considered for this component in case of successful completion of the courses.

Course materials and recommended reading

Basic literature:

1. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513.
2. Sample Penetration Testing Report URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
3. Sample Technical Penetration Report URL: https://tbgsecurity.
4. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-

Generic&gads_ad_group=OWASP&_gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE.
5. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
6. Yevseiev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseiev, 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

Additional literature:

7. Installing Metasploitable 2 URL: https://metasploit.help.rapid7.com/docs/metasploitable-2.
8. Build Metasploitable 3 URL: https://github.com/rapid7/metasploitable3.
9. Synergy of building cybersecurity systems: monograph / S. Yevseyev, 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
10. 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
11. 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.

Assessment and grading

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

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- credit test: 40% of the semester grade.

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 integrity and course policy

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 in academic groups with a lecturer, 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

28.08.2023 

Head of the department
Serhii YEVSEIEV

28.08.2023 

Guarantor of the educational program
Serhii YEVSEIEV