Syllabus
Course Program

Fundamentals of technical information protection

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
Profile, Selective

Semester
6

Language of instruction
English

Lecturers and course developers

Andrii Tkachov

andrii.tkachov@khpi.edu.ua
Candidate of Technical Sciences, senior researcher of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 60 publications, 25 articles in foreign publications and specialized publications of Ukraine, 6 patents for a useful model, guarantor of the educational and professional program of the first (bachelor) level of higher education. Leading lecturer in the disciplines: "Network Programming", "Development and Analysis of Algorithms", "Programming Technologies", "Programming Tools", "Web Security", "Fundamentals of Technical Information Protection", for undergraduate and graduate students.
More about the lecturer on the department's website

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 337, including 42 utility model patents, 17 monographs, of which 9 are collective monographs, 29 textbooks, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 156 articles in foreign publications and specialized publications of Ukraine, with 40 of them are in the Scopus scientometric database. Leading lecturer on 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 graduate students.
More about the lecturer on the department's website

General information

Summary

The educational discipline "Fundamentals of technical information protection" is an optional educational discipline. The discipline is aimed at acquiring skills in designing and creating a complex information protection system, the procedure for implementing information protection at information activity objects.

Course objectives and goals

Students' acquisition of the necessary basic knowledge regarding the procedure for creating complexes of technical protection of information at the objects of information activity.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control in the form of an exam.

Competencies

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-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.

Learning outcomes

LR-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LR-13. Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols.
LR-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.
LR-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.
LR-18. Use software and software-hardware complexes for the security of information resources.
LR-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LR-20. Ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
LR-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.
LR-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.
LR-23. Implement measures to prevent unauthorized access to information resources and processes in information and telecommunication (automated) systems.
LR-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).
LR-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.

LR-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.
LR-27. Solve problems of data flow protection in information and telecommunication (automated) systems.
LR-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.
LR-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.
LR-31. Apply protection theories and methods to ensure the security of elements of information and telecommunication systems.
LR-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.
LR-33. Solve the problems of ensuring the continuity of business processes of the organization on the basis of risk management theory.
LR-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.
LR-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.
LR-36. Detect dangerous signals of technical means.
LR-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.
LR-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.
LR-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.
RN–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.
LR-41. Ensure the continuity of the event and incident logging process based on automated procedures.
LR-42. Implement processes of detection, identification, analysis and response to information and/or cyber security incidents.
LR-43. Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents.
LR-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.
LR-45. Apply early classes of information security and/or cyber security policies based on risk-based access control to information assets.
LR-46. Analyze and minimize the risks of information processing in information and telecommunication systems.
LR-47. Solve the problems of protection of information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information.
LR-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.
LR-49. Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems.

LR-50. Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature).
LR-51. Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems.
LR-52. Use tools for monitoring processes in information and telecommunication systems.
LR-53. Solve problems of software code analysis for the presence of possible threats.

Student workload

The total volume of the course is 180 hours (6 ECTS credits): lectures - 36 hours, laboratory classes - 36 hours, self-study - 108 hours.

Course prerequisites

Information security of the state.

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. Basic concepts and categories.
Information security as a component of national security. Regulatory and legal provision of information security.
Topic 2. The concept of a technical channel of information leakage.
Organizational and technical measures for the technical protection of information at the facility.
Topic 3. Means and methods of detecting and blocking technical channels of acoustic information leakage.
Protection of information from leakage through technical channels formed by auxiliary technical means.
Topic 4. Cyber security and the security monitoring and management center (SOC).
Cyber Security and Security Monitoring and Control Center (SOC).
Topic 5. Windows operating system.
Ensuring the protection of end devices running Windows OS.
Topic 6. Overview of the Linux OS.
Basic tasks related to information security on a host running the Linux OS.
Topic 7. Ethernet and IP network protocols.
Ethernet and IP network protocols.
Topic 8. Network communication devices.
Network security infrastructure.
Topic 9. Hackers and their tools.
Common threats and attacks.
Topic 10. Network monitoring and monitoring tools.
Attacks on basic functions.
Topic 11. Approaches to network security protection.
Access control as a way to protect the network.
Topic 12. Use of data encryption and decryption tools.
Public key cryptography.

Topics of the workshops

This field is filled in the same way if the curriculum includes workshops.

Topics of the laboratory classes

Topic 1. Installing the CyberOps Workstation virtual machine.

Topic 2. Creating user accounts. Control and management of Windows system resources.
Topic 3. Navigating the Linux file system, setting permissions.
Topic 4. Study of intercepted TCP and UDP packets using the Wireshark program.
Topic 5. Study of DNS traffic. MySQL database attack.
Topic 6. Encryption and decryption of data using OpenSSL. Data encryption and decryption using fcrackzip.

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, prepare for laboratory work, control work and exam.

Course materials and recommended reading

Basic literature:

1. V.A. Khoroshko, A.A. Chekatkov. Methods and means of information protection.: K. - Junior, 2003. - 504 p.
2. The concept of technical information protection in Ukraine. CMU Resolution No. 1126 of 10/08/1997.
3. DSTU 3396.0-96. Information protection. Technical protection of information. Substantive provisions. Approved by the order of the State Standard of Ukraine dated 11.10.96 No. 423.
4. DSTU 3396.1-96. Protection of information. Technical protection of information. The order of work. Approved by the order of the State Standard of Ukraine dated 19.12.96 No. 511.
5. DSTU 3396.2-97. Protection of information. Technical protection of information. Terms and definitions. Approved by the order of the State Standard of Ukraine dated April 11, 1997 No. 200.
6. ND TZI 1.1-002-99. General provisions on the protection of information in computer systems against unauthorized access.
7. ND TZI 1.4-001-2000. A typical provision on the information protection service in an automated system.
8. ND TZI 3.7-003-2005 The procedure for carrying out works on the creation of a comprehensive information protection system in the information and telecommunications system.
9. ND TZI 3.3-001-07 "Protection of information at objects of information activity. Creation of a complex of technical protection of information. Procedure for development and implementation of information protection measures".
10. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.

Additional literature:

1. Regulation on state control over the state of technical protection of information dated 05/16/2007 No. 87.
2. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

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;
- exam: 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

17.01.2025 — Head of the department
Serhii YEVSEIEV

17.01.2025 — Guarantor of the educational program
Serhii YEVSEIEV