Syllabus
Course Program

Integrated information security systems

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
7

Language of instruction
English

Lecturers and course developers

Roman KOROLEV

roman.korolev@khpi.edu.ua
Candidate of economic sciences, associate professor of the department of cybersecurity of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 80, including 12 utility model patents, 1 collective monograph, 2 training manuals, 65 articles in foreign publications and specialized publications of Ukraine, 5 of them in the Scopus scientometric database. Leading lecturer in the disciplines: "Wireless and mobile security", "Fundamentals of steganography", "Business intelligence", "Physical foundations of technical means of intelligence" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Integrated information security systems" is a mandatory educational discipline. The discipline is aimed at students acquiring knowledge and skills that form the profile of a specialist in the field of information protection and cyber security of control systems in various fields.

Course objectives and goals

Teaching students the principles of building complex information protection systems based on the synthesis of organizational and technical measures to ensure the protection of information with limited access, the basics of electronic document management in the conditions of modern cyber threats and leakage through technical channels, ensuring the protection of information from unauthorized access based on the requirements of international information security standards , state regulatory documents on information protection technology.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - exam.

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 - 32 hours, laboratory classes - 16 hours, self-study - 72 hours.

Course prerequisites

Security in information and communication 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. Regulatory and legal provision of the organization of information protection at the objects of information activity.
Basic concepts in the field of cyber security, principles and components of national interests in the field of cyber security.
Topic 2 Technical protection of information.
Provisions on technical protection of information in Ukraine, basic provisions, procedure for carrying out work.
Topic 3. The procedure for the creation of KSZI in information and telecommunication systems (ITS).
General requirements for KSZI. The procedure for carrying out work on the creation of a comprehensive information protection system in the information and telecommunications system.
Topic 4. General provisions on the creation and attestation of complex technical information protection.
Creation of complexes of technical protection of information. Certification of complexes. Testing of the complex of technical protection of information.
Topic 5. Classification of automated systems. Standard functional profiles of information security against unauthorized access. Protection of information in computer systems against unauthorized access.
Types of automated systems. Standard functional profiles of information security against unauthorized access.
Topic 6. Threats of information in modern ICS, model of the offender and model of threats.
Classification of information threats in modern ICS. Types and procedure of developing a model of an offender and a threat model.
Topic 7. Formation of information security policy in IT.
Information security policy in the information and telecommunications system.
Topic 8. Stages of construction of KSZI, technical task for KSZI, act of certification of KSZI.
Basic principles of construction of KSZI.
Topic 9 Formation of the Information Protection Plan in ICS.
Provisions on the categories of objects where information with limited access, constituting a state secret, circulates.

Topics of the workshops

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

Topics of the laboratory classes

Topic 1. Concept, basic provisions of technical information protection. The order of work.
Study of the Regulation on technical protection of information in Ukraine, discussion of the main provisions, consideration of the procedure for conducting work on the certification of KSZI.
Topic 2. Information protection in computer systems. Development of an information protection plan.
Study of the Regulation on the protection of information in computer systems. Consideration of the procedure for developing the Information Protection Plan in computer systems.
Topic 3. Examination of the functionality of IT, formation of the task at KSZI.
Study of the algorithm for testing the functionality of the ITS. Development of the task at KSZI.
Topic 4. Development of security policy, technical task and project at KSZI.

Study of security policy. Consideration of the order of development of the technical task and the project at KSZI.
Topic 5. Criteria for evaluating the security of information in computer systems against unauthorized access. Development of an offender model and a threat model.
Development of an intruder model and a threat model in computer systems.

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. On the protection of information in information and telecommunication systems: Law of Ukraine dated 07.05.1994 No. 80/94-VR. Date of update: 12/31/2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. 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
3. 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
4. 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
5. 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
6. 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
7. DSTU 3396 0-96 Information protection. Technical protection of information. Basic provisions. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
8. 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
9. 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). https://tzi.com.ua/downloads/1.4-001-2000.pdf
10. ND TZI 2.5-004-99 Criteria for assessing 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). https://tzi.com.ua/downloads/2.5-004-99.pdf
11. 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). https://tzi.com.ua/downloads/2.5-005%20-99.pdf

12. 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.
13. 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).
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
14. 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.
https://zakononline.com.ua/documents/show/83554__83554
15. 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/
16. 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
17. 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 literature:

18. 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
19. 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
20. 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.
21. 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
22. 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
23. 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;
- 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

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV