Syllabus
Course Program

Organizational support for 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 training, Selective

Semester
7

Language of instruction
English

Lecturers and course developers

Olha KOROL

olha.korol@khpi.edu.ua
Candidate of technical sciences, associate professor, associate professor of the department of cyber security of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 150, of which 14 are textbooks, 48 articles in foreign publications and specialized publications of Ukraine, 8 patents for a useful model, 9 in the Scopus scientometric database. Leading lecturer in the disciplines: "Information security management", "State national security", "State information security", "Comprehensive training "Security of web applications"" for undergraduate and graduate 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

Educational discipline "Organizational support of information protection" is a selective educational discipline. The discipline is designed to acquire theoretical knowledge of information protection and practical skills in the organization of information protection. Students study the main directions, principles and conditions of organizational protection; basic approaches, requirements, methods and tools.

Course objectives and goals

The formation of theoretical knowledge regarding the analysis and assessment of threats to the information security of the object, the assessment of damages due to the illegal disclosure of restricted access information, the organization and maintenance of the regime of secrecy, selection, distribution and work with personnel.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control - credit test.

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
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.
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

Antivirus protection of information, Integrated information security systems, knowledge of working mechanisms with MS Word, MS Excel.

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. The task of organizational support for information protection.
The role of organizational measures in creating a reliable information protection mechanism. Tasks that are solved at the organizational level to ensure the security of information functioning.
Topic 2. Analysis and evaluation of threats to the object's information security.
Classification of information security threats by basic features. Three main types of threats.
Topic 3. Assessment of damages due to illegal disclosure of restricted access information and measures for its localization.
List of information with restricted access: state, commercial, banking, professional, official secrets, personal data and intellectual property. Overview of methods of unauthorized access. Conditions contributing to the improper possession of confidential information. Indicator of the criterion of the degree of absence or presence of material and moral damage caused to the object. Parameters of the cost of risk from the occurrence of an event.
Topic 4. Object security service.
The main tasks of the security service. Principles of the enterprise security system. Functions of the enterprise information protection service. List of units of the security service of the information processing facility or enterprise and their functions.
Topic 5. Selection, distribution and work with personnel.
Stages of the personnel selection procedure. Verification of personnel for reliability. The process of checking managerial personnel. Conclusion of contracts and confidentiality agreements. Peculiarities of dismissal of employees who have confidential information. Selection, allocation and work with security personnel. Observance of labor discipline and legality, strengthening of physical development, health, improvement of culture. Social protection of security personnel.
Topic 6. Organization and maintenance of secrecy regime.
Features of the secrecy regime. The procedure for organizing the secrecy regime. Closed works of secrecy mode. Documents regulating the work of units for the protection of state secrets. The rights of employees of units for the protection of state secrets. The main tasks of permanent technical commissions. The structure and content of the list of information constituting confidential information of the enterprise. The procedure for admitting employees to information constituting a commercial secret. The life cycle of documents containing trade secrets.
Topic 7. Organization of access, internal facility and fire protection regime.
Measures regulated by the access regime. Establishment of responsibility for ensuring access regime and preservation of material values in structural subdivisions. Documentation on access mode. Measures of internal object mode. Provision of fire protection regime.
Topic 8. Protection of information during accidents and other extreme situations.
Peculiarities of information influence in extreme conditions. Preventive measures. Issues that are resolved and documented when drawing up a preventive action plan. List of details of the action plan.
Topic 9. Ensuring the protection of information in the implementation of international scientific, technical and economic cooperation.
Channels of distribution of confidential information.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Templates of documents.
Topic 2. Creation of a structural grid of a document of a complex structure.
Topic 3. Using headers when creating document forms.
Topic 4. Use of styles in electronic documents.
Topic 5. Basics of creating documents with calculated details.

Topic 6. Automation of creation and distribution of documents of the same type.
Topic 7. Creation of lists of information with limited access.
Topic 8. Compilation and execution of organizational and administrative documents.
Topic 9. Keeping documents containing stamped information. Formation of cases.
Topic 10. Selection and transfer of documents for destruction.

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. About information: Law of Ukraine dated October 2, 1992 No. 2657-XII. Current edition dated 07/27/2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. On scientific and technical information: Laws of Ukraine dated June 25, 1993 No. 3322-XII. Current edition dated 04/19/2014. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
3. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. Current edition dated 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII // VVR of Ukraine. Current edition dated 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
5. On the protection of personal data: Law of Ukraine dated 09.02.2010 No. 2297–VI // VVR of Ukraine. Current edition dated 10/27/2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
6. Information protection in automated control systems: study guide / Compendium. I. A. Pilkevich, N. M. Lobanchykova, K. V. Molodetska. – Zhytomyr: Department of ZhDU named after I. Franka, 2015. – 226 p. URL: https://moodle.znu.edu.ua/pluginfile.php/1142772/mod_resource/content/1/Zahyst_informacii_ASU.PDF
7. On the approval of the General requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet of Ministers of Ukraine dated June 19, 2019 No. 518. Current edition dated September 7, 2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
8. Complex information protection systems: study guide / [Yaremchuk Yu.E., Pavlovsky P.V., Kataev V.S., Sinyugin V.V.] – Vinnytsia: VNTU, 2018. – 118 p. URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf
9. Loginova N. I. Legal protection of information: study guide / N. I. Loginova, R. R. Drobozhur. – Odesa: Phoenix, 2015. – 264 p. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/6dbd7fae-06f3-4afd-b2f7-871688668ea0/content
10. Ostapov S.E. Technology of information protection: study guide / S.E. Ostapov, S.P. Yevseev, O.G. Korol. – Kh.: Ed. HNEU, 2013. – 476 p. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf.

Additional literature:

1. Buryachok V.L., Tolyupa S.V., Semko V.V. Information and cyberspace: security problems, methods and means of combating: a guide. Kyiv. DUT-KNU, 2016. 178 p. URL: https://duikt.edu.ua/uploads/p_303_92597962.pdf

2. Yu.E. Yaremchuk Research of the combinational characteristics of domestic radio-opaque fabrics M1, M2 and M3 / Yu.E. Yaremchuk, V.S. Kataev, V.V. Sinyugin // Data registration, storage and processing. – 2015. – Volume 17. No. 3 – P. 56-65. URL: http://nbuv.gov.ua/UJRN/rzod_2015_17_3_8
3. Yaremchuk, Yu.E. Study of the characteristics of domestic radio-opaque fabrics H1, H2 and H3 with different combinations of their use / Yu.E. Yaremchuk, V.S. Kataev, M.Yu. Hyzhko, P.V. Pavlovsky // Registration , data storage and processing. – 2016. – Volume 18, No. 1. – P. 42-51. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34773/93691.pdf?sequence=2&isAllowed=y.

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

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV