Syllabus
Course Program

Fundamentals of Cybersecurity

Specialty
122 – Computer Science

Institute
Institute of Computer Science and Information Technology

Educational program
Computer Science and Intelligent Systems

Department
Software Engineering and Management Intelligent Technologies (321)

Level of education
Bachelor's level

Course type
Special (professional), Mandatory

Semester
6

Language of instruction
English, Ukrainian

Lecturers and course developers

Serhii Yevseiev

serhii_yevseiev@khpi.edu.ua
Doctor of Technical Sciences, Professor, Professor of the Department of Software Engineering and Information Technologies of NTU "KhPI"

Prepared and published more than 295 scientific and educational works (Google Scholar: https://scholar.google.com/citations?user=g-HezNwAAAAJ; ORCID https://orcid.org/0000-0003-1647-644; Scopus: https://www.scopus.com/authid/detail.uri?authorId=57190440690; Publons: https://publons.com/researcher/1527869/serhii-yevseiev/).
More about the lecturer on the department's website

General information

Summary

Acquaintance of students with the principles of building information security systems; acquaintance of students with the basic mechanisms of security services; study of information security management by students; teaching students the basics of information security audit; study of special mechanisms of cyber defense by students.

Course objectives and goals

Teaching students the principles of building information security systems, research and use of modern procedures for providing basic information security services in cyberspace, auditing the current state of information security.

Format of classes

Lectures, laboratory classes. Current control - laboratory work, intermediate modular control. Final control - exam.

Competencies

GC1. Ability to think abstractly, analyze and synthesize.
GC2. Ability to apply knowledge in practical situations.

GC3. Knowledge and understanding of the subject area and understanding of professional activities.
GC6. Ability to learn and master modern knowledge.
PC14. Ability to apply methods and tools to ensure information security, develop and operate special software to protect information resources of critical information infrastructure.

Learning outcomes

PLO15. Understand the concept of information security, the principles of secure software design, ensure the security of computer networks in conditions of incomplete and uncertainty of the source data.

Student workload

The total volume of the course is 90 hours (3 ECTS credits): lectures - 16 hours, laboratory classes - 32 hours, self-study - 42 hours.

Course prerequisites

Higher mathematics
Computer networks
Fundamentals of web development

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

Teaching and learning methods:
interactive lectures with presentations, discussions, laboratory classes, teamwork, case method, student feedback, problem-based learning.
Forms of assessment:
written individual assignments for laboratory work (CAS), assessment of knowledge in laboratory classes (CAS), express surveys (CAS), online tests (CAS), final/semester control in the form of a semester exam, according to the schedule of the educational process (FAS).

Program of the course

Topics of the lectures

Topic 1. The concept of cybersecurity of the state and components of national interests of Ukraine in cybersecurity
The main stages of internal audit on information security.
Topic 2. Cybersecurity risk analysis. Classification of cyber threats. Practical models of delimitation of access rights
Acquaintance with the main channels of information leakage. Basic principles of forming classifiers of computer incidents, cyber threats.
Topic 3. Mechanisms for ensuring the confidentiality and integrity of data
Basic mechanisms for ensuring integrity in information systems.
Topic 4. Authentication mechanisms
Basic special hash functions. Digital signature standards, their classification.
Topic 5. The main directions of development of modern cryptography
Methods of steganography in the spatial and frequency domain.
Topic 6. Mechanisms and protocols of key management in PKI
Basic PKI protocols based on symmetric and asymmetric cryptography.
Topic 7. Risk analysis technologies
Methods of risk analysis.
Topic 8. Risk analysis in non-information security management
Methods of risk analysis.

Topics of the workshops

Workshops are not provided within the discipline.

Topics of the laboratory classes

Topic 1. Deploy an operating system to audit the information security of computer networks and information systems
Topic 2. Tools for covertly collecting technical information from an information system or computer network
Topic 3. Research of modern block symmetric ciphers and encryption modes.
Topic 4. Research of electronic digital signature. El Gamal CPU, DSTU 4145, ECDSA. Investigation of system or network vulnerabilities using a specialized vulnerability scanner - Nessus
Topic 5. Steganography methods of information protection
Topic 6. Statistical studies of random and pseudorandom sequence generators according to the NIST method
Topic 7. Identify vulnerabilities in web resources and web applications. Vulnerability scanner - Vega
Topic 8. Collection of technical and sensory information with the help of class software - sniffers. A tool to study the vulnerabilities of wireless Wi-Fi networks - Aircrack-ng

Self-study

Individual assignments are not provided in the curriculum.
Students are recommended with additional materials (videos, articles) for self-study and processing.

Course materials and recommended reading

Key literature

1. Yevseev S.P., Ostapov S.E., Korol O.H. Cyber security: modern protection technologies. Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678.
2. R. V. Hryshchuk and Yu. G. Danyk. Fundamentals of cyber security: Monograph /; in general ed. Y. G. Dannyk. Zhytomyr: ZhNAEU, 2016.
3. I. S. Ivanchenko, V. O. Khoroshko, Yu. E. Khokhlacheva, and D. V. Chirkov under general ed. Prof. V. O. Khoroshka, "Ensuring the information security of the state", K: PVP "Zadruga", 2013.

Additional literature

4. Baranov A.A., Internet of things: theoretical and methodological foundations of legal regulation. Volume I. Fields of application, risks and barriers, problems of legal regulation, ISBN: 978-966-937-513-1, 2018, 344p.
5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
6. Edited by Serhii Yevseyev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p.
7. 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.
8. Doctrine of information security of Ukraine, approved by Decree of the President of Ukraine dated February 25, 2017 No. 47/2017. [Electronic resource]. Available: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.
9. Cybersecurity Strategy of Ukraine" (Enacted by the Decree of the President of Ukraine dated March 15, 2016 No. 96/2016).

Assessment and grading

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

100% final assessment in the form of exam (36%) and current assessment (64%).
36% exam
64% current rating:
Module №1 (12%)
Module №2 (12%)
Laboratory work (40%)
Laboratory work № 1 (5%)
Laboratory work № 2 (5%)
Laboratory work № 3 (5%)
Laboratory work № 4 (5%)
Laboratory work № 5 (5%)
Laboratory work № 6 (5%)
Laboratory work № 7 (5%)
Laboratory work № 8 (5%)

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	08.06.2023	Head of the department Ihor HAMAIUN
	08.06.2023	Guarantor of the educational program Andrii KOPP