Syllabus
Course Program

Information systems and Internet technologies

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
6, 7

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

General information

Summary

The educational discipline "Information systems and Internet technologies" is a mandatory educational discipline. The discipline is aimed at acquiring knowledge about the technological and methodical foundations of the structure of modern information systems (IS); mastering the skills of using IS (with elements of cyber security), which ensure the effective work of users in a modern information environment.

Course objectives and goals

Formation of theoretical knowledge of the basic principles of building information systems using modern Internet technology - HTTP protocol, hypertext markup language HTML, Java Script, Java, PHP, Python, SQL database. Formation of practical skills in the design, creation, construction, debugging, deployment and maintenance of modern information systems (with elements of cyber security).

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control in the form of an test (6th semester), exam (7th semester).

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

LR-1. Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
LR-2. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;
LR-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.

LR-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.
LR-5. Adapt under the conditions of frequent changes in the technologies of professional activity, to predict the final result.
LR-6. Critically understand the main theories, principles, methods and concepts in education and professional activity.
LR-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.
LR-8. Prepare proposals for regulatory acts on ensuring information and/or cyber security.
LR-9. Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents.
LR-10. Perform analysis and decomposition of information and telecommunication systems.
LR-11. Perform analysis of connections between information processes on remote computer systems.
LR-12. Develop threat and intruder models.
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-15. Use modern hardware and software of information and communication technologies.
LR-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.
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.
PH-30. Assess the possibility of unauthorized access to elements of information and telecommunication systems.
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.

LR-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 240 hours (8 ECTS credits): lectures - 40 hours, laboratory classes - 56 hours, self-study - 144 hours.

Course prerequisites

Basics of programming, Programming technologies.

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. Work on the Internet.
Fundamentals of Hypertext Transfer Protocol (HTTP).
Topic 2. Basics of HTML.
Semantic structure of the page, HTML tags.
Topic 3. Work with forms.
Passing parameters through forms.
Topic 4. Basics of CSS.
CSS selectors. Properties.
Topic 5. Creating a page layout and layout.
Adaptive design.
Topic 6. Working with the browser.
Browser Object Model. Working with the Document Object Model.
Topic 7. Data storage and data exchange technologies.
Fundamentals of database design.
Topic 8. SQL. Database management and administration.
Built-in SQL functions.
Topic 9. Queries to the database.
Work with databases.
Topic 10. Creation of client-server applications.
Pattern model-representation-controller.
Topic 11. Modern frameworks.
Design patterns.
Topic 12. Development of information systems.
Protection of client-server applications.

Topics of the workshops

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

Topics of the laboratory classes

Topic 1. Work on the Internet. Fundamentals of Hypertext Transfer Protocol (HTTP).
Topic 2. Basics of HTML. Semantic structure of the page, HTML tags.
Topic 3. Working with forms. Transferring parameters through forms.
Topic 4. Basics of CSS. CSS selectors. Properties.
Topic 5. Creating a page layout and layout. Adaptive design.
Topic 6. Working with the browser. Browser Object Model. Working with the Document Object Model.

Topic 7. Data storage and data exchange technologies. Fundamentals of database design.
Topic 8. SQL. Database management and administration. Built-in SQL functions.
Topic 9. Queries to the database. Work with databases.
Topic 10. Creation of client-server applications. Pattern model-representation-controller.
Topic 11. Modern frameworks. Design patterns.
Topic 12. Development of information systems. Protection of client-server applications.

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 credit test or exam.

Course materials and recommended reading

Basic literature:

1. Information protection technologies./ S.E. Ostapov, S.P. Yevseiev, O.G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
2. WEB technologies [Electronic resource]: Educational reference manual / S.P. Yevseiev, A.M. Tkachov, V.O. Alexiev, Yu.M. Ryabukha – Kharkiv: KHNEU named after S. Kuznetsia, - Lviv: "New World -2000" Publishing House, 2021. - 390 p.
3. Academy of web development MDN [Electronic resource]. – Access mode: https://developer.mozilla.org/.
4. HTML Tutorial [Electronic resource]. – Access mode: https://www.tutorialspoint.com/html/index.htm.
3. CSS Tutorial [Electronic resource]. – Access mode: https://www.tutorialspoint.com/css/index.htm.
5. Javascript Tutorial [Electronic resource]. – Access mode: https://www.tutorialspoint.com/javascript/index.htm.
SQL Tutorial [Electronic resource]. – Access mode: https://www.tutorialspoint.com/sql/index.htm.

Additional literature:

1. Tutorials Library [Electronic resource]. – Access mode: https://www.tutorialspoint.com/index.htm.
2. Ethernet technology: laboratory workshop / M. O. Bilova, S. P. Yevseiev, O. S. Zhuchenko, I. S. Ivanchenko, O. V. Shmatko.– Lviv: "Novyi Svit-2000", 2020. - 196 p.
3. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
4. 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.
5. 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.

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 or 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