Syllabus
Course Program

Systems engineering

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
8

Language of instruction
English

Lecturers and course developers

Stanislav MILEVSKYI

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

Author of more than 100 scientific and educational and methodological works. Scientific Guarantor of the educational and scientific program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Fundamentals of Mathematical Modeling of Security Systems", "English in Academic Applications", "Modeling of Cyber-Physical Actions" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The curriculum of the discipline "Systems engineering" determines the content and scope of knowledge necessary for a specialist in the field of development and implementation of complex engineering systems. The discipline covers the issues of development, analysis and life cycle management of complex systems, starting from conceptual design to their operation and disposal. Particular attention is paid to the use of modern tools for modeling, analysis and optimization of engineering systems. Laboratory classes help students consolidate the acquired knowledge in practice.

Course objectives and goals

The purpose of studying the discipline is the formation of future specialists in the knowledge and skills necessary for the design, development and implementation of complex technical systems taking into account the requirements of reliability, safety and efficiency.

Format of classes

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

Competencies

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-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.).

Learning outcomes

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-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-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-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-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.

Student workload

The total volume of the course is 90 hours (3 ECTS credits): lectures - 24 hours, laboratory classes - 12 hours, self-study - 54 hours.

Course prerequisites

Higher mathematics, Fundamentals of mathematical modelling of security 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. Introduction to system engineering.
Basic concepts and definitions. Life cycle of systems. System requirements.
Topic 2. System engineering processes.
Life cycle models. Requirements management. Analysis and evaluation of alternatives.
Topic 3. A systematic approach to design.
Conceptual design. Synthesis and analysis of decisions. Modeling of systems.
Topic 4. Evaluation of performance and reliability of systems.
Basics of reliability. Risk analysis. Evaluation of operational characteristics of systems.
Topic 5. Modeling and simulation in system engineering.
Modeling methods. Tools for simulation. Applied modeling problems.
Topic 6. System engineering project management.
Project planning and organization. Execution control and risk management.
Topic 7. Integration of systems.
Approaches to integration. Testing and verification of systems. Compatibility requirements.
Topic 8. Life cycle of systems.
Support, modernization and utilization of systems. Economic analysis and life cycle cost assessment.
Topic 9. Configuration management.
Version control. Change management. Configuration support.
Topic 10. Modern trends in system engineering.
Global trends in automation, cyber-physical systems, artificial intelligence in systems engineering.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Fundamentals of system modeling.
Topic 2. Development of a conceptual model of the system.
Topic 3. Modeling and simulation of dynamic systems.
Topic 4. Assessment of system reliability.
Topic 5. Risk analysis in the project.
Topic 6. Integration of subsystems into complex systems.
Topic 7. Management of system requirements.
Topic 8. Using configuration management tools.
Topic 9. Project management using specialized tools.
Topic 10. Verification and validation of 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. Blanchard, Benjamin S. Systems Engineering and Analysis. Pearson Education, 2013. https://books.google.com.ua/books/about/Systems_Engineering_and_Analysis.html?id=tC-pBwAAQBAJ&redir_esc=y
2. Sage, Andrew P., and James E. Armstrong. Introduction to Systems Engineering. Wiley, 2000. https://books.google.com.ua/books/about/Introduction_to_Systems_Engineering.html?id=of4VEAAAQBAJ&redir_esc=y
3. Stevens, Richard, Peter Brook, Ken Jackson, and Stuart Arnold. Systems Engineering: Coping with Complexity. Pearson Education, 1998. https://www.scenarioplus.org.uk/reviews/stevens.htm

Additional literature:

4. INCOSE. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Wiley, 2015. https://download.e-bookshelf.de/download/0003/6422/62/L-G-0003642262-0007580512.pdf
5. Maier, Mark W., and Eberhardt Rechtin. The Art of Systems Architecting. CRC Press, 2009. http://ndl.ethernet.edu.et/bitstream/123456789/38076/1/43.pdf
6. Wasson, Charles S. System Engineering Analysis, Design, and Development: Concepts, Principles, and Practices. Wiley, 2015. https://lib.manaraa.com/books/System%20Analysis%20Design%20%201209577.pdf.

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