Syllabus
Course Program

Modeling of socio-cyberphysical systems

Specialty
113 Applied mathematics

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Intelligent Data Analysis

Department
Cybersecurity

Level of education
Bachelor's level

Course type
Special (professional), Selective

Semester
5

Language of instruction
Ukranian

Lecturers and course developers

Oleksandr MILOV

oleksandr.milov@khpi.edu.ua
Doctor of technical sciences, professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 200 scientific and educational and methodological works. Academic supervisor for protected candidate theses, guarantor of the educational and professional program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Mathematical foundations of cryptology and cryptanalysis", "Data structures", "Industrial and office espionage", "Digital forensics", for undergraduate and graduate students, Section "Methodology of scientific and pedagogical activity in the sciences of cyber protection" for postgraduate students.
More about the lecturer on the department's website

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 educational discipline "Modeling of socio-cyberphysical systems" is an optional educational discipline. The educational discipline is devoted to the fundamental principles of the theory of

mathematical and computer modeling of socio-cyber-physical systems, the principles of building and researching mathematical models of socio-cyber-physical systems.

Course objectives and goals

Training of specialists in the field of information security, security of telecommunications support, and mobile devices, as well as specialists in modeling of socio-cyber-physical systems, based on mastering the principles and methods of collecting digital information for researching the behavior of agents of security systems, conducting static analysis of individual and group behavior of participants of socio-cyber-physical systems , using tools and methods of various areas of cyber security.

Format of classes

Lectures, laboratory classes, calculation tasks, consultations. Final control – exam.

Competencies

GC 2. Ability to apply knowledge in practical situations.
GC 7. Ability to search, process and analyze information from various sources.
GC 8. Knowledge and understanding of the subject area and understanding of professional activities.
GC 10. Skills in the use of information and communication technologies.
SC 2. Ability to perform tasks formulated in mathematical form.
SC 5. Ability to develop algorithms and data structures, software tools and program documentation.
SC 6. Ability to design databases, information systems and resources.
SC 7. Ability to solve professional problems with the help of computer equipment, computer networks and the Internet, in the environment of modern operating systems, using standard office applications.
SC 9. Ability to use modern technologies for programming and testing software.
SC 13. Ability to search, systematically study and analyse scientific and technical information, domestic and foreign experience related to the use of mathematical methods to study various processes, phenomena and systems.
SC 14. Ability to understand the task formulated in the language of a particular subject area, to search and collect the necessary initial data.

Learning outcomes

LO 7. Be able to conduct practical research and find a solution incorrect tasks.
LO 8. Combine methods of mathematical and computer modeling with informal expert analysis procedures to find optimal solutions.
LO 9. To build efficient computing and sustainability systems, performance and system resource consumption algorithms for numerical researching mathematical models and solving practical problems.
LO 10. To have methods for choosing rational methods and algorithms for solving mathematical problems of optimization, operations research, optimal management and decision-making, data analysis.
LO 11. Be able to apply modern programming technologies and software development, software implementation numerical and symbolic algorithms.
LO 14. Demonstrate the ability to self-learn and continue professional development.
LO 15. Be able to organize your own activities and get results within a limited time frame.
LO 16. Demonstrate skills of interaction with other people, ability to work in a team.
LO 17. To be able to collect, process, analyse, systematize scientific and technical information, while avoiding academic dishonesty.

Student workload

The total volume of the course is 180 hours (6 ECTS credits): lectures - 32 hours, laboratory classes - 32 hours, self-study - 116 hours.

Course prerequisites

“Mathematical Analysis, Computer discrete mathematics, Basics of cryptology, Programming.

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.
Goals and objectives of the educational discipline "Modeling of socio-cyberphysical systems". The place of the discipline in the training process of a cyber security specialist. The structure and content of the thematic plan for studying the discipline; educational and methodical literature. Peculiarities of studying the discipline; forms of control of students' knowledge, abilities and skills. Directions of scientific research work of students.
Topic 2. Modeling.
Basic concepts of modeling, concepts of systems and models, main types of models, types of models and their classification according to various criteria, requirements for models.
Topic 3. Basic types of modeling. Formal methods of building models.
The main types of modeling (analytical, simulation, statistical), their characteristics and their relationship with each other. Formal methods of building models: cybernetic approach, system dynamics, theoretical-multiple approach.
Topic 4. Principles of building models. Modeling technology.
The main principles of building models: information sufficiency, expediency, feasibility, multiplicity of models, aggregation, parameterization, application of the iterative multilevel modeling methodology. Modeling technology: main stages, their relationship and characteristics.
Topic 5. Identification of mathematical model parameters. Adequacy, sensitivity, consistency of the model.
Setting the identification task, the main stages of its solution and their relationship. Concepts of adequacy, sensitivity and consistency of the model, formal methods of their verification.
Topic 6. Structured approaches to information gathering.
Open source intelligence methods. Overview of methods of structured analysis.Types of information collected: Business information (financial, customers, suppliers, partners).
Information about IT infrastructure. Identification of sources of information.
Topic 7. Basic concepts and definitions used in the description of security models of computer systems.
Elements of the theory of computer security. Entity, subject, access, information flow. Classic classification of information security threats. Types of information flows. Types of access and information flow management policies. Leakage of access rights and violation of CS security. Mathematical foundations of security models.
Topic 8. System-dynamic models in socio-cyber-physical systems. The language of system dynamics.
The concept of system dynamics. Classification of systems. Methods of studying complex systems. System analysis and system dynamics. Conceptual apparatus. Basic concepts. Types of connections between system elements. Classification and designation of model elements.
Topic 9. System-dynamic models in socio-cyber-physical systems. Construction of simulation models.
Formation of research goals. Collection of information about the system and processes (reference stage). Building a conceptual model. Building a machine model. Conducting simulation experiments and model verification. Discussion of the model (debriefing). Model improvement.
Topic 10. Theoretical game models of behavior in socio-cyberphysical systems.
Elements of game theory. Games and their classification. Pure player strategies. Mixed strategy players. Matrix games. Minimax strategies. Saddle point game. A game without a saddle point. Solving the matrix game. Optimality criteria of the administrator's strategy.Methods of solving matrix games. Dominance. Using linear programming. Bimatrix games. Nash equilibria in a finite game of N people. The prisoner's dilemma. Software for finding game solutions.
Endless games.
Topic 11. Application of game theory for modeling socio-cyberphysical systems.

An example of a matrix game "attacker - administrator". Software application for choosing the optimal set of protection tools. Representation of attacks in cyberspace. Choosing an effective means of protection against DoS/DDoS attacks. Modeling the behavior of a gambling criminal.
Topic 12. Agent models of socio-cyber-physical systems.
Objects and agents. Classification of agents of cyber-physical systems. Multiagent systems. Interaction of agents in cyberspace. Communication and coordination of cyber-physical agents. Cooperation and confrontation of agents. Models of conflict situations in cyberspace.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Using the MATLAB system for modeling socio-cyberphysical systems.
Topic 2. Using the SIMULINK system for modeling socio-cyber-physical systems.
Topic 3. Modeling finite state machines as prototypes of cyberspace agents.
Topic 4. Modeling of socio-cyber-physical systems by Petri nets.
Topic 5. Basics of building system-dynamic models using PowerSim. Construction of a simulation model of "attacker-defender" interaction.
Topic 6. Construction and use of the game model "Repelling attacks in cyberspace".

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 exam.

Course materials and recommended reading

References

1. Cyber-Physical Systems / ed. by G. M. Siddesh et al. Chapman and Hall/CRC, 2015. URL: https://doi.org/10.1201/b19206 (date of access: 31.01.2023).
2. Industrial Cloud-Based Cyber-Physical Systems / ed. by A. W. Colombo et al. Cham : Springer International Publishing, 2014. URL: https://doi.org/10.1007/9783-319-05624-1 (date of access: 31.01.2023).
3. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. https://lira-k.com.ua/preview/12867.pdf
5. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
6. Nardelli P. H. J. Cyber-Physical Systems: Theory, Methodology, and Applications. Wiley & Sons, Incorporated, John, 2022 https://content.e-bookshelf.de/media/reading/L-18316928-9cb3bd7865.pdf

Additional references

1. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
2. 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

3. 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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
4. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ крипографічного захисту / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. Євсеєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
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: 30% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 20% 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	Date, signature 29.08.2024		Head of the department Serhii YEVSEIEV
	Date, signature 29.08.2024		Guarantor of the educational program Olena AKHIIEZER