Syllabus
Course Program

Fundamentals of mathematical modelling of security systems

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
5

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 educational discipline "Fundamentals of mathematical modelling of security systems" is a mandatory educational discipline. The discipline is aimed at acquiring skills in the field of system modeling, mastering the methods of simulation modeling using the package (PowerSim).

Course objectives and goals

Formation of students' theoretical knowledge on the basics of modeling security systems, students' assimilation of the main approaches and principles of building models and the acquisition of skills in their application to solve modeling problems that arise in the development of information systems and security systems.

Format of classes

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

Competencies

GC-1. Ability to apply knowledge in practical situations.
GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-4. Ability to identify, state and solve problems in a professional manner.
GC-5. Ability to search, process and analyze information.
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

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 - 16 hours, laboratory classes - 32 hours, self-study - 72 hours.

Course prerequisites

Higher mathematics, Operating system architecture and security, Mathematical foundations of cryptology.

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. Modeling. Basic concepts. Types of models, their classification. Requirements for models.
Concept of modeling, concept of system and model, main types of models, types of models and their classification according to various criteria, requirements for models.
Topic 2. 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 3. 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 model adequacy, sensitivity and non-contradiction, formal methods of their verification.
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. 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. Basic concepts. The concept of an automaton. Elements of graph theory. Algorithmically solvable and algorithmically unsolvable problems. Lattice model. The main types of formal security models. The problem of the adequacy of the implementation of the security model in a real computer system.
Topic 6. Models of computer systems with discretionary access control.
Access matrix model of Harrison-Ruzzo-Ullman. Model description. Security analysis of KhRU systems. A model of a typified access matrix. Take-Grant access rights distribution model. Basic provisions of the classic Take-Grant model. Advanced Take-Grant model. Submission of Take-Grant systems by KhRU systems. Discretionary DP models. Basic DP model. DP model without cooperation of trusted and untrusted subjects.
Topic 7. Models of an isolated software environment.
Subject-oriented model of an isolated software environment. Correctness of subjects in DP-models of CS with discretionary access control. DP model with entities functionally associated with subjects. DP model for secure administration policy. DP model for the policy of absolute separation of administrative and user powers. DP model with entities functionally or parametrically associated with subjects. Application of the FAS DP model for the analysis of the security of web systems. Methods of preventing leakage of access rights and implementation of prohibited information flows. A method of preventing the possibility of obtaining the right of access to the possession of an untrusted subject to a trusted subject. A method of implementing a secure administration policy. A method of implementing the policy of absolute separation of administrative and user powers.
Topic 8. Models of computer systems with mandated access control.
Bela-LaPadula model. Classic Bela-LaPadula model. An example of an incorrect definition of security properties. Low-watermark policy in the Bela-LaPadula model. Examples of implementation of prohibited information flows. Security of transitions. Weeb's Information Integrity Mandate Policy Model. Model of military communication systems. General provisions and basic concepts.
An informal description of the SBS model. A formal description of the SBS model. Mandatory DP model. Rules for transforming states of the mandated DP model. Security in the sense of Bela-LaPadula. Conditions for raising the access level by the subject.
Topic 9. Security models of information flows.
Automatic model of security of information flows. Software model of information flow control. A probabilistic model of security of information flows. DP-models of security of information flows over

time. DP model with blocking access of trusted subjects. Mandatory DP model with blocking access of trusted subjects. Mandatory DP model with identification of generated subjects. Mandated DP-model of CS implementing a policy of strict mandated access management.
Topic 10. Models of computer systems with role-based access control.
The concept of role-based access management. Basic model of role-based access management. Role-based access management administration model. Substantive provisions. Administration of multiple authorized user roles. Administer the set of access rights that roles have. Role hierarchy administration. A model of mandated role access management. Protection against the threat of confidentiality of information. Protection against threats to confidentiality and integrity of information. Mandatory essence-role DP model of access and information flow management in operating systems of the Linux family. System status. Functionally or parametrically associated entities. Access and access rights. Mandatory access management tasks for system states. The task of mandated integrity control for system states. Actual possession. State conversion rules.
Topic 11. Models of interaction in cyber security.
Lotka-Volterra model. Classification of types of interactions. Competition. Predator-prey. Kolmogorov's model.

Topics of the workshops

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

Topics of the laboratory classes

Topic 1. Automatic models. Petri net model.
Topic 2. Models of system dynamics.
Topic 3. Discrete-time models.
Topic 4. Structural security models.
Topic 5. Simulation models.
Topic 6. Modeling of computer systems with discretionary access control.
Topic 7. Models of an isolated software environment.
Topic 8. Models of computer systems with mandated access control.
Topic 9. Security models of information flows.
Topic 10. Models of computer systems with role-based access control.
Topic 11. Models of interaction 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. Bakhrushin V.E. Mathematical modeling: a study guide [Text] – Zaporizhzhia: GU "ZIDMU", 2004. – 140 p.
http://moodle.nati.org.ua/mod/resource/view.php?id=7442
2. Zhernovy Yu.V. Simulation modeling of mass service systems: Workshop / Yu.V. Zhernovy. — Lviv: Ed. center of LNU named after I. Franka, 2007. — 307 p.

https://new.mmf.lnu.edu.ua/wp-content/uploads/2018/02/Imit_model.pdf
3. Mathematical modeling of systems and processes: teaching. manual / P. M. Pavlenko, S. F. Filonenko, O. M. Cherednikov, V. V. Treytyak. - K.: NAU, 2017. - 392 p.
https://pdf.lib.vntu.edu.ua/books/2020/Pavlenko_2017_392.pdf
4. Mathematical modeling of telecommunication systems and networks: training manual [Text] / E.M. Chernykhivskyi. – Lviv: Publishing House of Lviv Polytechnic, 2011. – 272 p.
https://vlp.com.ua/node/7158
5. O. V. Makhney Mathematical modeling: study guide / O. V. Makhney. — Ivano-Frankivsk: V. P. Suprun, 2015. — 372 p.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/matmod_content.pdf
6. Tomashevsky V.M. Modeling of systems / V.M. Tomashevskyi. — K.: BHV Publishing Group, 2005. — 352 p.
https://pdf.lib.vntu.edu.ua/books/2016/Tomashev_2005_352.pdf
7. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. 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. URL:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional literature:

10. O. V. Makhnei Mathematical support for automation of applied research / O. V. Makhnei, T. P. Goy. — Ivano-Frankivsk: Simyk, 2013. — 304 p.
https://kdrpm.pnu.edu.ua/wp-content/uploads/sites/55/2018/03/Maple_content.pdf
11. Pavlenko P. M. Fundamentals of mathematical modeling of systems and processes: science. manual - K.: NAU Book Publishing House, 2013. - 201 p.
https://er.nau.edu.ua/bitstream/NAU/24750/1/%D0%A2_%D0%9F%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0 %BA%D0%BE%20%D0%9F.%D0%9C._%D0%9D%D0%B0%D0%B2%D1%87.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