Syllabus
Course Program

Mathematical foundations of artificial intelligence

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
5

Language of instruction
English

Lecturers and course developers

Serhii POHASII

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

The number of scientific publications: more than 95, including 2 utility model patents, 6 monographs, of which 4 are collective monographs, 4 teaching aids, 4 of which bear the seal of the Ministry of Education and Science of Ukraine, 65 articles in foreign publications and specialized publications of Ukraine, with 11 of them are in the Scopus scientometric database. Leading lecturer in the disciplines: "Analog and digital electronic devices", "Internet of things and services", "Security of cloud technologies", "Fundamentals of construction and protection of modern operating systems", "Modeling of critical infrastructure systems", "Fundamentals of construction and protection of microprocessor systems ", "Security of smart technologies and Internet of things", "Information and communication systems in the field of national security" for undergraduate and graduate students, Section "Information security of cloud services", "Modern methods of protection of socio-cyber-physical systems", "Modeling of mechanisms cyber security" for graduate students.

More about the lecturer on the department's website

General information

Summary

The course "Mathematical Foundations of Artificial Intelligence" covers the basic mathematical concepts and methods underlying modern algorithms and artificial intelligence (AI) systems. Students will study areas such as linear algebra, probability and statistics, mathematical analysis, optimization, and graph theory that are essential to understanding machine learning algorithms, neural networks, decision making, and data processing. Laboratory classes help students consolidate the acquired knowledge in practice.

Course objectives and goals

The purpose of the educational discipline "Mathematical foundations of artificial intelligence" is to provide students with theoretical and practical knowledge of the mathematical foundations necessary for understanding and developing methods and algorithms of artificial intelligence.

Format of classes

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

Competencies

GC-2. Knowledge and understanding of the domain and understanding of the profession.
GC-5. Ability to search, process and analyze information.
PC-2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.
PC-9. Ability to perform professional activities based on the implemented information and/or cyber security management system.

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-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-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-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-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-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-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-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 90 hours (3 ECTS credits): lectures - 16 hours, laboratory classes - 16 hours, self-study - 58 hours.

Course prerequisites

Higher mathematics, Fundamentals of mathematical modeling 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 mathematical methods in artificial intelligence.
Overview of key mathematical sections used in AI. The role of mathematics in the development of machine learning models
Topic 2. Linear algebra for artificial intelligence.
Vectors, matrices, operations on them. Eigenvectors, eigenvalues, singular matrix decomposition (SVD).
Topic 3. Probability and statistics in AI.
Basics of probability distributions. Conditional probabilities, Bayesian networks, laws of large numbers
Topic 4. Theory of decision-making based on probabilities.
Bayes theory and its application in AI. Forecasting based on probabilistic models
Topic 5. Mathematical analysis and its application in AI.
Derivatives, gradients, integrals. Gradient Descent: Basics and Modifications (Stochastic, Mini-Batch) Modeling methods. Tools for simulation. Applied modeling problems.
Topic 6. Graph theory and algorithms on graphs.
Basic concepts of graphs: vertices, edges, degrees. Graph search algorithms and their use in artificial intelligence
Topic 7. Numerical methods in AI problems.
Basics of numerical linear algebra. Methods for solving linear systems and least squares
Topic 8. Mathematical foundations of optimization.
Optimization problems in machine learning. Gradient descent and optimization acceleration methods (Newton's method, momentum)
Topic 9. Regularization methods in machine learning.
L1 and L2 regularization. The problem of overtraining and combating it with regularization
Topic 10. Basics of information theory and entropy.
Definition of information and entropy. Cross-entropy, Kullback-Leibler divergence and their use in AI algorithms.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1 Basics of working with linear algebra.
Operations with vectors and matrices. Eigenvalues and expansions of matrices.
Topic 2. Modeling of random events using probabilistic methods.
Calculation of conditional probabilities. Implementation of Bayesian networks
Topic 3. Gradient descent.
Implementation of gradient descent for the minimization problem. Study of algorithm variants (stochastic, mini-batch)
Topic 4. Optimization methods.
Practical application of optimization methods in model training tasks. Implementation of minimum search algorithms
Topic 5 Numerical methods.
Solving problems using the method of least squares. Numerical methods for solving systems of linear equations.
Topic 6 Modeling on graphs.
Implementation of basic algorithms on graphs. Visualization and analysis of graph structures
Topic 7 Practice of building a neural network.
Building a simple neural network using libraries (eg TensorFlow, PyTorch)
Model training and analysis of results
Topic 8 Clustering and regression.
Implementation of clustering and regression algorithms on real data. Evaluation and visualization of model results.

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. Hlybovets A. M., Gulaeva N. M. Evolutionary algorithms. M. - K.: NaUKMA, 2013., 828p. URL:
2. Kononyuk A.Yu. Neural networks and genetic algorithms - K.: "Korniichuk", 2008. - 446 p. URL: https://pdf.lib.vntu.edu.ua/books/2016/Kononyk_2008_470.pdf
3. Mathematical apparatus of artificial intelligence in electric power systems: textbook / V.V. Kyryk. - Kyiv: KPI named after Igor Sikorskyi, "Polytechnic" ed. - 2019.-224 p. URL: https://ela.kpi.ua/server/api/core/bitstreams/34259dab-7eaa-4b78-86d9-4a000d90b2be/content.

Additional literature:

1. Lytvyn, V.V. Intellectual systems / V.V. Lytvyn - Lviv: Novy svit-2000. - 2009. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Intelektual_system.pdf
2. Methods and systems of artificial intelligence: Study guide for students of the field of training 6.050101 "Computer science" / Comp. : A.S. Savchenko, O. O. Synelnikov. - K.: NAU, 2017. – 190 p. URL: https://er.nau.edu.ua/bitstream/NAU/40676/1/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%20%D1%82%D0%B0%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8%20%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83%20_%D0%9D%D0%B0%D0%B2%D1%87_%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD.pdf
3. Rudenko O. G., Bodyanskyi E. V. Artificial neural networks: Training manual. — Kharkiv: SMIT Company LLC, 2006. — 404 p. URL: https://f.eruditor.link/file/260293/
4. Subbotin S.O. Representation and processing of knowledge in artificial intelligence systems and decision support. Zaporizhzhia: ZNTU, 2008. — 341 p. URL: https://eir.zp.edu.ua/server/api/core/bitstreams/63742fdf-b5e4-46e2-83b4-561d97c2cffe/content

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

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV