Syllabus
Course Program

Machine Learning in Cybersecurity

Specialty
113 Applied mathematics

Institute
Educational and Scientific Institute of Computer Science and Information Technology.

Educational program
Intelligent Data Analysis

Department
Department of Computer Mathematics and Data Analysis.

Level of education
Bachelor's level

Course type
Special (professional), Mandatory.

Semester
8

Language of instruction
Ukranian

Lecturers and course developers

Oleksii Haluza

oleksii.haluza@khpi.edu.ua
Doctor of Science (Physics&Mathematics), Full Professor, Professor of Computer Mathematics and Data Analysis Department.

Work experience – more than 20 years. The author of many scientific, educational, and methodological works. Leading lecturer in the courses: «Algorithmization and Programming», «Optimization Methods», «Machine Learning», etc.

More about the lecturer on the department's website

General information

Summary

The course is dedicated to studying advanced methods and algorithms of machine learning applied to cybersecurity. Students will become familiar with the basics of threat analysis and the application of artificial intelligence methods for detecting, identifying, and neutralizing cyber threats in real-world conditions. The course covers techniques for anomaly detection and malware analysis; the use of deep learning algorithms in cybersecurity; methods for protecting machine learning models from adversarial attacks; issues of privacy, ethical aspects, and data security.

Course objectives and goals

The goal of the course is to train specialists capable of developing modern solutions for protecting information systems using machine learning technologies.

Format of classes

Lectures, laboratory classes, consultations, self-study. Final control in the form of an exam.

Competencies

GC 1. Ability to learn and master modern knowledge.

GC 2. Ability to apply knowledge in practical situations.
GC 3. Ability to generate new ideas (creativity).
GC 4. Ability to be critical and self-critical.
GC 6. Capability of abstract thinking, analysis and synthesis.
GC 7. Ability to search, process and analyse 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 1. Ability to use and adapt mathematical theories, methods and techniques to prove mathematical statements and theorems.
SC 3. Ability to choose and apply mathematical methods for solving applied problems, modelling, analysis, design, management, forecasting, decision-making.
SC 4. Ability to select and apply numerical methods to solve optimization problems.
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 20. Ability to develop and operate software tools for intelligent analysis of measurement and observation data, texts, signals and images.

Learning outcomes

LO 1. Demonstrate knowledge and understanding of basic concepts, principles, theories of applied mathematics and use them on practice.
LO 2. To know the basic principles and methods of mathematical, complex and functional analysis, linear algebra and theory numbers, analytic geometry, theory of differential equations, in particular partial differential equations, probability theory, mathematical statistics and random processes, and numerical methods.
LO 10. To have methods for choosing rational methods and algorithms for solving mathematical optimization problems, research operations, optimal management and decision-making, and data analysis.
LO 12. Solve individual engineering problems and/or tasks that arise in at least one subject area: sociology, economy, ecology, and medicine.
LO 24. Be able to apply existing and develop new algorithms and software tools for processing measurement and observation data, texts, signals and images.
L0 25. Be able to apply modern information technologies and software for processing large amounts of data based on distributed and cloud services.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures – 20 hours, laboratory classes – 20 hours, self-study – 80 hours.

Course prerequisites

"Methods and Tools of Machine Learning", "Blockchain: Basics and Application Examples", "Anomaly Detection in Data and Time Series", "Intrusion Detection", "Optimization Methods".

Features of the course, teaching and learning methods, and technologies

In teaching this discipline, methods such as gamification and peer-to-peer learning are employed. Learning management systems (LMS) are used throughout the educational process.

Program of the course

Topics of the lectures

Topic 1: Overview of Modern Cybersecurity Threats.

Cyber threats and incidents: current trends and new types of attacks. Introduction to cyberattack analysis using machine learning. The role of ML in attack protection: active defense and detection.

Topic 2: Advanced Anomaly Detection Methods in Cybersecurity.

Algorithms and methods: Isolation Forest, Autoencoders, LSTM. Application of unsupervised and semi-supervised learning methods for attack detection. Features of network traffic data and event logs.

Topic 3: Deep Learning for Cybersecurity Tasks.

Application of convolutional and recurrent neural networks for network data and log analysis. LSTM and GRU for real-time threat prediction and detection. Autoencoders for anomaly detection: methodology and examples.

Topic 4: Application of ML for Malware Analysis.

Malware classification using deep neural networks. PE file analysis: using neural models and feature extraction methods. Exploration of dynamic and static malware analysis techniques.

Topic 5: Generation of Adversarial Examples and Protection of ML Models.

Attacks on machine learning models: examples of adversarial attacks. Methods for protecting models: resilience to adversarial examples, data-level, and model-level defenses. Neural network attacks and defenses in the context of cybersecurity.

Topic 6: Machine Learning for Phishing and Malicious Website Detection.

ML for website classification: analysis of phishing sites. Feature selection for webpage analysis: textual data, URL structure, metadata. Building models for automatic filtering of malicious websites.

Topic 7: User Behavior Analysis and Insider Threat Detection.

Behavioral analytics using machine learning. Building user profiles and detecting deviations. Examples of ML application for protecting against insider threats.

Topic 8: Application of Reinforcement Learning in Cybersecurity.

Fundamentals of reinforcement learning and its use in attack detection tasks. RL for automatic adaptation of intrusion detection systems (IDS). Examples of RL application for dynamic cybersecurity configuration.

Topic 9: Attack Detection Based on Network Traffic Analysis.

Using clustering and classification methods for network traffic analysis. Time series analysis for real-time attack detection (e.g., DDoS). Building models for traffic anomaly detection and packet analysis.

Topics of the workshops

Workshops are not included within the framework of this discipline.

Topics of the laboratory classes

Topic 1: Anomaly Detection Using Autoencoders.
Topic 2: Application of LSTM for Attack Detection in Network Traffic.
Topic 3: Malware Classification Based on PE File Analysis.
Topic 4: Adversarial Attacks on ML Models.
Topic 5: Phishing Website Detection Using Machine Learning Methods.
Topic 6: Insider Threat Detection Through Behavioral Analysis.
Topic 7: Application of Reinforcement Learning for Adaptive Security.
Topic 8: Anomaly Detection in Network Traffic Using Time Series.
Topic 9: Building an IDS System Using ML Methods.
Topic 10: Analyzing the Robustness of Neural Network Models Against Adversarial Attacks.

Self-study

The course involves completing individual assignments, the results of which are automatically checked using LMS tools and monitored and evaluated by instructors. Students are also recommended additional materials (videos, articles) for independent study.

Non-formal education

As part of non-formal education in accordance with the relevant regulation (http://surl.li/pxssv), the educational component or its individual topics may be considered in cases of independent completion of professional courses/training, obtaining civic education, online education, professional internships, etc.

Course materials and recommended reading

Basic literature

1. Кононова К. Ю. Машинне навчання: методи та моделі: підручник. – Харків: ХНУ ім. В. Н. Каразіна, 2020. – 301 с. ISBN: 978-966-285-654-5
https://karazin.ua/storage/static-content/source/documents/vydavnytstvo/2021/navchalni-vydannia/Kononova .pdf
2. M. Omar. Machine Learning for Cybersecurity. - Springer Cham, 2022. - 480 p.
https://doi.org/10.1007/978-3-031-15893-3
3. T. Bhardwaj, H. Upadhyay, T. K. Sharma, S. L. Fernandes. Artificial Intelligence in Cyber Security: Theories and Applications. - Springer Cham, 2024. - 138 p.
https://doi.org/10.1007/978-3-031-28581-3

Additional literature

1. T. Sipola, T. Kokkonen, M. Karjalainen. Artificial Intelligence and Cybersecurity. - Springer Cham, 2022. – 301 p. https://doi.org/10.1007/978-3-031-15030-2
2. N. Nedjah, A. A. Abd El-Latif, B. B. Gupta, L. M. Mourelle. Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities. - Springer Cham, 2022. - 262 p.
https://doi.org/10.1007/978-3-030-96737-6

Internet resources

1. https://en.wikipedia.org/wiki/Machine_learning
2. https://en.wikipedia.org/wiki/Computer_security

Assessment and grading

Criteria for assessment of student performance, and the final score structure

100% of the final grade consists of assessment results in the form of an exam (40%) and ongoing assessment (60%).

Exam: written assignment (2 theoretical questions and a problem) and an oral presentation.

Ongoing Assessment: grades for laboratory work, 2 control tests, and a calculation task.

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 Olena AKHIIEZER
	Date, signature 29.08.2024		Guarantor of the Educational Program Olena AKHIIEZER