Syllabus
Course Program

Internet science. Navigation in complex 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
Profile training, Selective

Semester
6

Language of instruction
English

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

Iryna AKSONOVA

Iryna.Aksonova@khpi.edu.ua
Candidate of Economic Sciences, Associate Professor of the Department of Cyber Security of National Technical University "Kharkiv Polytechnic Institute".

The number of scientific publications: more than 150, including certificates of authorship - more than 15, chapters in monographs - 10, articles referenced in the scientific metric databases Scopus and WoS - 9. Lecturer in the disciplines: "Modeling of information security systems", "Artificial intelligence and business analytics", "Standardization and certification in the field of information security", "Technology of business process security management" and others for undergraduate and graduate students.
More about the lecturer on the department's website

General information

Summary

The study of the discipline is aimed at the understanding and active use of two directions that are actively developing at the present time — the theories of information search and complex networks. It is at the junction of these two areas that the solution to the open problem of effective navigation in modern information networks may lie.

Course objectives and goals

To form a system basic idea, primary knowledge, skills and skills of students from the basics of the theory of information search in complex communication and information systems, mastering the concept of in-depth analysis of texts — Text Mining, which included technological and methodological approaches of content analysis, computer linguistics, in particular, approaches to solving such tasks as automatic abstracting, analysis of interrelationships of concepts, construction of searchable images of documents, issues of cluster analysis of arrays of text documents, consideration of characteristics that take into account not only topology, but also statistical distributions of characteristics of nodes and connections in complex networks . In general, the goal of the discipline is as follows - to systematically outline the state of existing theoretical and technological possibilities, provide possible prospects for development, give impetus to new ideas in the field of online information search.

Format of classes

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

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-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-8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.
PC-10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
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 - 24 hours, laboratory classes - 12 hours, self-study - 84 hours.

Course prerequisites

Algorithms and data structures.

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.
Topic 2. Modern information networks.
Internet - history and protocols. World Wide Web - World Wide Web. Peer networks. Problems of Internet content development
Topic 3. Information search.
Boolean search model. Classic Boolean model. Extended Boolean model. Fuzzy search model. Vector spatial model search. Probabilistic search model. Search algorithms in peering networks. Resource search algorithm by keys. The method of broad primary search. The method of random wide primary search. Intelligent search engine. "Most results from the past heuristics" methods. The "random walk" method. Information and search languages. Characteristics of information search.
Topic 4. The concept of text mining.
Content analysis. Elements of Text Mining. Extracting concepts. Definition of interrelationships of concepts. Automatic referencing. Search images of documents. Detection of duplication of information. Detection of new events. Implementation of systems with Text Mining elements
Topic 5. Information classification methods.
Classification task. Formal description of classification problems. Ranking and clear classification. Linear classification. The Rocchio method. Regression method. DNF-classifier. Classification based on artificial neural networks. Bayesian classifier. The method of support vectors. Evaluation of classification quality
Topic 6. Elements of cluster analysis.
Latent semantic analysis. The k-means method. Hierarchical grouping-unification. Method of suffix trees. Hybrid methods. Ranking of search results.
Topic 7. Empirical distributions and mathematical formalism.
Empirical regularities. Degrees of distribution of random variables.Homogeneous functions and scaling. Order parameter and phase transitions.
Topic 8. Entropy and amount of information.
Shannon entropy. Properties of entropy. Conditional entropy. Entropy of a continuous source of information. Amount of information. Mutual information.
Topic 9. Fundamentals of the theory of complex networks.
Complex network settings. Model of weak ties. Model of small worlds. WWW as a complex network. Visualization of complex networks.
Topic 10. Elements of percolation theory.
Tasks of percolation theory. Characteristics of percolation networks. A network with exponentially wide distribution. Diode percolation networks. Percolation on random networks. Theory of percolation and simulation of attacks on networks.
Topic 11. Models of information flows.
Linear models. Exponential model. Logistic model. Information diffusion model. A model of self-organized criticality.
Topic 12. Elements of fractal analysis.
Fractals and fractal dimension. Abstract fractal. Information space and fractals. Fractals and time series. Multifractal analysis of series of measurements.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Building a pain model of information search.

Topic 2. Phono-semantic analysis of information.
Topic 3. Content analysis of texts.
Topic 4. Text Mining. Classification of texts and messages.
Topic 5. Basics of clustering. The k-means method.
Topic 6. Basics of clustering. Hierarchical clustering.
Topic 7. Calculations of entropy characteristics of messages.
Topic 8. Visualization of complex networks.
Topic 9. Building models of information flows.
Topic 10. Construction of fractal models and analysis of time series.

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

References

1. Analysis of data and knowledge: study guide / V.V. Lytvyn, V.V. Pasichnyk, Yu.V. Nikolskyi – Lviv: Magnolia-2006, 2021. – 276 p.
https://library.nuft.edu.ua/analiz-danyh-ta-znan/
2. Data Mining: searching for knowledge in data / A. Ya. Gladun, Yu. V. Rogushina – K.: LLC "VD "ADEF-Ukraine", 2016. – 452 p.
https://nvd-nanu.org.ua/c41aa335-1dce-4dcb-6f6a-9ccd7313ce84/
3. Fox G.C. From Computational Science to Internetics: Integration of Science with Computer Science, Mathematics and Computers in Simulation, Elsevier, 54 (2000) 295-306.

Additional references

4 Lyubun Z. M. Basics of the theory of neural networks / Z. M. Lyubun /: Lecture text. – Lviv: Ivan Franko LNU Publishing Center, 2007. – 142 p.
https://f.eruditor.link/file/236389/
5. Intellectual data analysis: a study guide / A. O. Oliynyk, S. O. Subbotin, O. O. Oliynyk. – Zaporizhzhia: ZNTU, 2012. – 278 p.
https://eir.zp.edu.ua/server/api/core/bitstreams/71efb3db-bf4c-43c0-bc33-b4449efd1c68/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: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- credit test: 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 28.08.2024	Head of the department Serhii YEVSEIEV
	Date, signature 28.08.2024	Guarantor of the educational program Serhii YEVSEIEV