Syllabus
Course Program

Fundamentals of steganographic information protection

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
7

Language of instruction
Ukrainian

Lecturers and course developers

Roman Korolev

roman.korolev@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 40, including 1 textbook, 23 articles in foreign publications and specialized publications of Ukraine, 10 patents for a useful model. Leading lecturer in the disciplines: "Physical foundations of technical means of intelligence", "Fundamentals of steganographic information protection", "Corporate networks and access systems", "Security and auditing of wireless and mobile networks".

More about the lecturer on the department's website

General information

Summary

The educational discipline "Fundamentals of Steganographic Information Protection" is a mandatory educational discipline. The discipline is aimed at students' acquisition of skills and principles of construction, implementation and application of steganographic systems and protocols, the ability to apply methods, algorithms and tools for evaluating steganoresistance and other qualitative indicators of steganosystems and steganographic protocols.

Course objectives and goals

Getting students the necessary basic knowledge of digital steganography, which is used to hide the fact of the existence of information and create watermarks. Special attention is paid in the course to the study of the problems of using digital steganography in the modern information space, analysis of attacks on steganograms and assessment of stability.

Format of classes

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

Competencies

GC 1. Ability to learn and master modern knowledge.
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 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 8. Ability to operate and maintain software of automated and information systems for various purposes.
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 solutions to incorrect problems.
LO 8. Combine mathematical and computer modeling methods with informal expert analysis procedures to find optimal solutions.
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 14. Show the ability to self-learn and continue professional development.
LO 15. To be able to organize own activities and obtain results within a limited time.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 30 hours, laboratory classes - 30 hours, self-study - 60 hours.

Course prerequisites

“Fundamentals 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. Digital steganography.
The structure and content of the discipline, its connection with other disciplines of the curriculum. Subject, terminology, field of use.
Topic 2. Mathematical model of steganosystems.
Steganographic protocols. Practical aspects of data embedding.
Topic 3. Main areas of practical use of steganographic methods of information protection.
Classification of steganographic systems and stegocontainers.
Topic 4. Peculiarities of the human visual system.
The main properties of the human visual system used in hiding data in images.
Topic 5. Digital formats of still images.
BMP, GIF, TIFF, JPEG formats. Features of computer image processing.
Topic 6. Hiding data in a spacious area of images.
A method of hiding in the least significant bit of data.
Topic 7. Hiding data in the frequency domain of images. Koch and Zhao method.
Hiding confidential information in the frequency set of the image.
Topic 8. Features of the human auditory system.

The main properties of the human auditory system used in hiding data in audio signals. Digital formats of audio signals (WAV, WMA, MP3, AAC, OGG Vorbis formats). Features of computer processing of audio signals.

Topic 9. Digital watermarks.

A generalized model of the digital watermarking system. Classification of digital watermarking system.

Topic 10. Digital prints.

Terminology and basic provisions. Statistical registration of the print. Scheme of asymmetric fingerprint registration.

Topic 11. Covert channels in computer systems and networks.

Hidden channels in operating systems. Hiding data in executable files. The concept of kleptrography.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Software means of steganographic protection of information.
Topic 2. Work with Steganos Security Suite steganographic information protection program.
Topic 3. Hiding data in the spatial domain of images using the least significant bit method.
Topic 4. Hiding data in the spatial domain of images by the permutation method.

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. Yevseev S.P. Cybersecurity: modern protection technologies. Lviv: Novyi Svit-2000, 2019. - 678. - Access mode:
http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Kuznetsov O.O. Steganography: a textbook / O.O. Kuznetsov, S.P. Yevseev, O.G. Korol - Kh.
http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/2289/1/%d0%a1%d1%82%d0%b5%d0%b3%d0%b0%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d0%b8%d1%8f.pdf
3. Khoroshko VO Computer steganography: a textbook / VO Khoroshko, YE Yaremchuk, VV Karpinets - Vinnytsia: VNTU, 2017. - 155 p.
https://learn.ztu.edu.ua/pluginfile.php/272322/mod_resource/content/1/Xoroshko_Komputer_2017_155.pdf.
4. Kozyura V.D. Information security in computer systems: textbook / V.D. Kozyura, V.O. Khoroshko, M.E. Shelest - Nizhyn: FOP Lukianenko V.V., TPK “Orhidea”, 2020. - 236 p.
http://ir.stu.cn.ua/bitstream/handle/123456789/19248/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B2%20%D0%BA%D0%BE%D0%BC%D0%BF.%20%D1%81%D0%B8%D1%81.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5. Konakhovych H.F. Computer steganographic processing and analysis of multimedia data: textbook / H.F. Konafovych, D.O. Prohonov, O.Y. Puzyrenko - K. - “Alex Print Center”, 2018/ - 558 p.
https://books.google.com.ua/books?id=-clcDwAAQBAJ&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Additional references

6. Evseev S. P. Cybersecurity: Laboratory workshop on the basics of cryptographic protection. - Lviv “Novyi Svit-2000”, 2020. - 241 p. - Access mode:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

7. Evseev S.P. Cybersecurity: Cryptography with Python: a textbook. - Lviv “Novyi Svit-2000”, 2021. - 120 p. - Access mode:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Evseev S. P. Cybersecurity: basics of coding and cryptography / S. P. Evseev, O. V. Milov, S. E. Ostapov, O. V. Severinov: Novyi Svit-2000 Publishing House, 2023. 657 p. - Access mode:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others: PC TECHNOLOGY CENTER, 2021. - 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others: PC TECHNOLOGY CENTER, 2023. - 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others: PC TECHNOLOGY CENTER, 2022. - 196 p.
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: 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	Date, signature		
	29.08.2024		Head of the department Serhii YEVSEIEV
	Date, signature 29.08.2024		Guarantor of the educational program Olena AKHIIEZER