Syllabus
Course Program

Basics of steganographic information protection

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
7

Language of instruction
English

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 80, including 12 utility model patents, 1 collective monograph, 2 training manuals, 65 articles in foreign publications and specialized publications of Ukraine, 5 of them in the Scopus scientometric database. Leading lecturer in the disciplines: "Wireless and mobile security", "Fundamentals of steganography", "Business intelligence", "Physical foundations of technical means of intelligence" for undergraduate and graduate students.

More about the lecturer on the department's website

General information

Summary

The educational discipline "Basics 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, consultations, self-study. Final control - credit test.

Competencies

GC-1. Ability to apply knowledge in practical situations.
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-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-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-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-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-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-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 150 hours (5 ECTS credits): lectures - 32 hours, laboratory classes - 32 hours, self-study - 86 hours.

Course prerequisites

Basics of cryptographic protection, 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. 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

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

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, 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. 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 literature:

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;
- 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

28.08.2024 — Head of the department
Serhii YEVSEIEV

28.08.2024 — Guarantor of the educational program
Serhii YEVSEIEV