Syllabus of the educational component
Program of educational discipline

Fundamentals of cryptographic protection

Code and name of specialty
125 – Cyber security and information protection

Institute
National Institute of Computer Sciences and Information Technologies (320)

Educational program
Cyber security

Department
Cyber security (328)

Level of education
Bachelor

Type of discipline
Special (professional), Mandatory

Semester
5

Language of teaching
English

Professor, developer

Milov Oleksandr Volodimirovich
Oleksandr.Milov@khpi.edu.ua

Doctor of technical sciences, professor of the cyber security department of NTU "KhPI".

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.

Learn more about the teacher on the department's website

General information

Annotation

The educational discipline "Fundamentals of cryptographic protection" is a mandatory educational discipline. The discipline is aimed at studying symmetric and asymmetric methods of information encryption, their use; types of cryptanalysis and the possibility of its application.

Purpose and objectives of the disciplines

Acquaintance with the theoretical foundations of cryptology; acquisition of skills in practical use, formulation and solving of information encryption problems; understanding the essence of information processes in cryptographic systems; use of computers to solve encryption and decryption problems; development and use of mathematical and computational models of information encryption processes, their optimization and development of improvement directions.

Format of classes

Lectures, laboratory work, independent work, consultations. Final control - credit.

Competences

GC 1. Ability to apply knowledge in practical situations. KZ 2. Knowledge and understanding of the subject area and understanding of the profession.
GC 4. Ability to identify, pose and solve problems according to professional direction KZ 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 2. Ability to use information and communication technologies, modern methods and models of information security 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 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins.
PC 7. The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, 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 10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.
PC 11. Ability to monitor the 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 one's 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. To adapt in 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 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. pH-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 transfer protocols.
LO-14. Solve the task of protecting programs and information processed in information and telecommunication systems by means of hardware and software 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 protection systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
LO-17. To ensure the processes of protection 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 protection 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 protection of information resources.
LO-19. Apply theories and methods of protection to ensure information security in information and telecommunication systems.
LO-20. To 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 in accordance with the established security policy in information and information and telecommunication (automated) systems.
LO-22. To solve the problems of management of 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 information and telecommunications (automated) systems.

LO-24. Solve the problems of managing access to information resources and processes in information and 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 information and telecommunication (automated) systems using event registration logs, their analysis and established 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 the problems of data flow protection in information, information and telecommunication (automated) systems.
LO-28. Analyze and evaluate the effectiveness and level of security of resources of various classes in information and information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security. RN-29. To 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 in 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 established security policy.
LO-33. To solve the problems of ensuring the continuity of business processes of the organization on the basis of risk 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 protection systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established 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 protection processes and determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information protection 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 protection 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 protection 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. To solve the problems of ensuring the continuity of the organization's business processes on the basis of risk theory and the established information security management system, in accordance with domestic 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 protecting 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. RN-54. To 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.

Scope of the discipline

The total scope of the discipline is 180 hours. (6 ECTS credits): lectures – 48 hours, laboratory work – 32 hours, independent work – 100 hours.

Prerequisites for studying the discipline (prerequisites)

Mathematical foundations of cryptology, Security in ICS, Higher mathematics (special chapters).

Features of the discipline, methods and technologies of education

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, individual group projects, and master classes are used as teaching methods aimed at activating and stimulating the educational and cognitive activity of applicants.

Program of educational discipline

Topics of lectures

Topic 1. Theoretical foundations of information protection.
Basic concepts. Models of secret systems. The main tasks of the security system. Symmetric and asymmetric cryptosystems. Modes of operation of symmetric cryptosystems.
Topic 2. Protocols of authenticity. Digital signature.
Mechanisms of authenticity. Classification of digital signature. Hashing methods. Authentication mechanisms based on the use of software and hardware. Kerberos authentication. Topic 3. Strict authentication protocols.
Classification of methods 2 FA. Authentication confidence levels. Threats to 2 FA. Two-factor authentication in Linux.
Topic 4. PGP system.
Main functions of the system. Classification of keys. Mechanisms for ensuring authenticity and confidentiality. Trust system.
Topic 5. Basics of PKI technology.
Main functions and composition of technology. Physical and logical topology. Cryptoperiod. The main mechanisms of technology based on symmetric and asymmetric cryptosystems.

Topic 6. SSL, TLS integrity protocols.
Interconnection of critical infrastructure objects with cyber-physical systems. Structure of SSL, TLS protocols. Functions of the SSL protocol. ATTACKS ON SSL/TLS.
Topic 7. Basics of post-quantum cryptography.
Basic concepts. The basis of quantum computing. Basic algorithms of quantum cryptanalysis. Topic 8. Basics of theories of information and coding.
The general structure of the communication system. Models of a binary symmetric channel without memory. Efficient Huffman coding. Error correction and invention. Classification of binary codes. Basic concepts of the theory of interference-resistant coding. Fields of Galois. The structure of the finite fields of their properties. Bowes-Choudhury-Hockingham codes.
Topic 9. Basics of decoding. Berlekamp-
Massey algorithm. Example.
Topic 10. Post-quantum algorithms based on McAlis and Niederreiter crypto-code constructions. Hybrid protection systems based on loss-making codes.
Classification of crypto-code structures. Elliptic curves. Basics of construction (formation of key matrices, formation of a cryptogram). Stability assessment. Ways to reduce the capacity of key data. Formation of crypto-code constructions on algebraic-geometric (elliptic) codes. Basics of cryptography on lossy codes. Formation of hybrid crypto-code structures.

Topic 11. Stream symmetric cryptosystems.
Symmetric cryptosystems. RC-4 stream cipher. Stability. Initialization of the S-block. PRC-4A stream cipher. STRUMOK stream cipher. Stream cipher SNOW2.0.

Topics of practical classes

Practical work within the discipline is not provided.

Topics of laboratory work

Topic 1. The simplest ciphers.
Topic 2. Study of the properties of the operating modes of block ciphers.
Topic 3. Exploring authentication and privacy protocols using RSA. Topic 4. Study of digital signature protocols.
Topic 5. Study of PGP system protocols. Topic 6.
Steganographic methods of information protection.
Topic 7. NIST STS methodology for evaluating statistical properties of cryptographic algorithms. Topic 8. Construction of cyclic codes.
Topic 9. Work with qubits. Emulation of measurements.

Independent work

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 assessment.

Literature and educational materials

Basic literature:

1. Yevseyev S.P. Cyber security: modern protection technologies. / Evseev S.P., Ostapov S.E., Korol O.G. // Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678. - Access mode: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasnitekhnolohii-zakhystu.pdf.
2. Yevseyev S.P. Information protection technologies. Multimedia interactive electronic edition of combined use / comp. S. P. Yevseev, O. G. Korol, S. E. Ostapov, G. P. Kots - Kh. S. Kuznetsia, 2016. – 1013 Mb. ISBN 978-966-676-624-6.
3. Bonaventure O. Computer Networking: Principles, Protocols and Practice. – Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. – 272 p.

4. O. O. Kuznetsov, S. P. Yevseev, S. V. Kavun, and O. H. Korol Signals and codes. Algebraic methods of synthesis. Monograph. Kharkiv, Ukraine: Ed. HNEU, 2009.
5. O. O. Kuznetsov, S. P. Yevseev, and S. V. Kavun Information protection and economic security of the enterprise. Monograph. Kharkiv, Ukraine: Ed. HNEU, 2009.
6. C. P. Yevseev, O. Yu. Yokhov, and O. G. Korol Data hashing in information systems. Monograph. Kharkiv, Ukraine: Ed. HNEU, 2013.
7. Yevseev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p.
8. Information protection technologies./ S.E. Ostapov, S.P. Yevseev, O.G. King. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.

Additional literature:

1. Yevseyev S.P. CYBER SECURITY: LABORATORY PRACTICE ON THE FUNDAMENTALS OF CRYPTOGRAPHIC PROTECTION / S.P. Yevseev, O.V. Milov, O.G. Korol - Lviv: "New World-2000", 2020. - 241 p.
2. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.
3. Edited by Serhii Yevseyev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p.
URL:https://www.researchgate.net/publication/352013398_Synergy_of_building_cybersecurity_systems_Monograph.
4. A. Rukhin, J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2000.

Evaluation system

Criteria for evaluating student performance and distribution of points

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: 40% of the semester grade

Rating scale

Sum points	National assessment	ECTS
90–100	Perfectly	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactorily	D
60–63	Satisfactorily	E
35–59	Unsatisfactorily (additional required study)	FX
1–34	Unsatisfactorily (need to repeat study)	F

Norms of academic ethics and policy of the course

The student must adhere to the "Code of Ethics of Academic Relations and Integrity of NTU "KhPI": show discipline, education, benevolence, honesty, responsibility. Conflict situations should be openly discussed in study groups with the teacher, and if it is impossible to resolve the conflict, it should be brought to the attention of the employees of the institute's directorate. Regulatory and legal support for the implementation of the principles of academic integrity of NTU "KhPI" is posted on the website:http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Coordination

Syllabus agreed

Head of the department

28.08.2023		Serhii Yevseyev
28.08.2023		Guarantor OP Olga KOROL