Syllabus of the educational discipline
«INFORMATION PROTECTION IN COMPUTER SYSTEMS»

Cycle of Higher Education	*First cycle of higher education (Bachelor's degree)*
Field of Study	*12 Information Technologies*
Specialty	*123 Computer engineering*
Educational program	*Computer systems and networks*
Discipline status	*Normative*
Teaching language	*English*
Year of studies, semester	*3 year (6 semester)*
Number of credits ECTS	*4.5 credits*
Distribution by types of trainings and hours of study	*Lectures, Laboratory studies, Independent training*
Form of final assessment	*Exam*
Teacher	*Korol Yu.Yu., associate professor of the department of computer systems and network*
Teacher's contacts	*yuriy.korol@uzhnu.edu.ua*
Course Schedule	*According to the timetable*

The purpose of studying the discipline "Information Protection in Computer Systems" - familiarization with organizational, technical algorithmic and other methods and tools of information protection, legislation and standards in this area, with modern cryptosystems.

As a result of studying the discipline the student must:

know:

- features of information as an object of protection, the list and features of the main threats to information in computer systems, approaches to developing a security policy for computer systems, basic principles of information protection, the order of forming a set of information protection tools, the principles of access control to protected resources of a computer system, cryptographic methods and means of protecting information, methods and means of protecting information from leakage by technical channels, the procedure for determining the requirements for information protection in a computer system

be able to:

- apply mathematical methods to describe and study cryptosystems; assess the cryptographic strength of ciphers; conduct experiments, data collection and modeling in computer systems

- analyze the security features of computer systems and networks. Conduct random attacks on security features to find vulnerabilities and solve existing problems.

Prerequisites for learning

Programming, Discrete Mathematics, Linear Algebra and Analytic Geometry, Information and Coding Theory, Probability Theory and Mathematical Statistics, Computer Logic

Content of the educational discipline

Topic 1. Fundamentals of information protection in the CS
Topic 2. Basic attack patterns and organization of information leakage channels
Topic 3. Organization of information security systems
Topic 4. Mathematical models of discretionary security policy
Topic 5. Mathematical models of mandate access policy
Topic 6. Organizational and technical tasks of information protection
Topic 7. Passwords. User identification and authentication
Topic 8. Biometric identification and authentication
Topic 9. Fundamentals of cryptographic protection of information
Topic 10. Classic symmetric cryptosystems.
Topic 11. Symmetric encryption
Topic 12. Stock ciphers and ciphers with variable key length
Topic 13. PRS generators
Topic 14. Asymmetric cryptographic systems

Topic 15. Electronic digital signature. Message authentication
Topic 16. Key management
Topic 17. Fundamentals of cryptanalysis: basic principles
Topic 18. Cryptographic package CrypTool
Topic 19. Steganography

Course page on the Moodle platform (personal training system)	*Syllabus of the educational discipline, hyperlinks to electronic publications of the discipline, recommended literature, students' attendance, lecture materials, presentations, questions for self-control, methodical materials for laboratory works, tests, tasks for checking students' knowledge.* https://moodle.uzhnu.edu.ua

Recommended literature

1. *Bruce Schneier Secrets and Lies: Digital Security in a Networked World. - Wiley; 1st edition, 2015. - 450p.*
2. *Bruce Schneier Applied Cryptography: Protocols, Algorithms and Source Code in C. - Wiley; 1st edition, 2015. - 784p.*
3. *Bruce Schneier Cryptography Engineering: Design Principles and Practical Applications. - Wiley; 1st edition, 2010. - 384p.*

Assessment system of learning outcomes

The ECTS grade that a student receives after studying a credit module of a discipline is determined according to the student's rating. A student's credit module rating consists of the points the student receives during the semester for the following types of work:
1. Modular control work (MCW) duration of 2 acad. hours each. The maximum number of points for the MCW is 40 points.
2. Performance of laboratory works.
During the semester, students perform 8 laboratory works
Scores on individual and independent work of students are awarded for: preparation of essays, modernization of tasks, creative approach to task performance, performance of tasks to improve didactic materials on the discipline: 0-10 points for each module.
Each module is assessed a maximum of 100 points. At the end of the discipline a rating score is derived as the arithmetic average of the points from the two modules.

ECTS and national grading scale

Mark scale	ECTS	Exam	Test
90 - 100	A	Excellent	Satisfied
82 - 89	B	Good	
74 - 81	C		
64 - 73	D	Satisfactory	
60 - 63	E		
35 - 59	FX	"Unsatisfactory" with possibility to pass the exam again	"Not satisfied" with possibility to pass the exam again
1 - 34	F	"Unsatisfactory" with obligatory repeated study of the discipline	"Not satisfied" with obligatory repeated study of the discipline