BASICS OF INFORMATION SECURITY

COURSE SYLLABUS ABSTRACT

Specialty 1-28 01 02 Electronic Marketing

	STUDY MODE		
	full-time	part-time	part-time (shortened program)
Year	2	3	–
Semester	4	5	–
Lectures, hours	34	8	–
Practical classes (seminars), hours	16	4	–
Pass/fail, semester	4	5	–
Contact hours	50	12	–
Independent study, hours	58	96	–
Total course duration in hours / credit units	108/3		

1. Course outline

The aim of the discipline is to teach students the basic methods of information security, information protection means, modern hardware and software algorithms of information encryption, building reliable information storage systems, as well as studying prospective directions in the development of modern means of information security.

2. Course learning outcomes

The objectives of the discipline are: studying threats to information security; study of methods and tools of information protection; gaining knowledge of the principles of organization and construction of integrated information security systems.

As a result of mastering the discipline, a student must

know: basic concepts of information security; requirements to information protection systems; principles of building information protection systems; basic algorithms of information encryption; methods of authenticity check of information process components

be able to: design the structure and choose the components of data protection systems; apply methods and tools of computer information protection; evaluate the reliability of computer information protection methods

Know: skills to assess reliability of computer information protection methods; methodology for information process component authentication; technology for information security of computer systems.

3. Competencies

SK-1 Ensure the security of information, taking into account how it is represented and the offender model

4. Requirements and forms of midcourse evaluation and summative assessment: credit