Syllabus of the course

"Program and data security"

Specialty	*121 Software engineering*
Study Program	*Software engineering*
Level (Bachelor, Master, PhD)	*the first (Bachelor) level of higher education*
Course status	*mandatory*
Teaching language	*English*
Intended stage in the study program	*4 year, 7 semester*
Number of ECTS credits	*5*
Workload	*Lectures – 24 hours.*
	Tutorials – 0 hours.
	Laboratory studies – 36 hours.
	Self study – 90 hours.
Assessment method	*Grading*
Department	*Department of Cyber Security and Information Technologies, Kharkiv, 9-A Nauky Ave. 057-702-18-31, http://www.kafcbit.hneu.edu.ua/*
Teaching staff Course coordinator	*Semenov Serhiy, Doctor of Engineering Sciences, Professor;* *Starkova Olha, Doctor of Engineering Sciences, Professor.*
Contacts of teaching staff	*serhii.semenov@hneu.net* *olha.starkova@hneu.net*
Office hours	*Lecture: according : according to the schedule* *Laboratory classes: according to the schedule*
Course schedule	*At the Department of Cybersecurity and Information Technologies, full-time, according to the schedule of consultations, individual*

Learning objectives and skills

to teach students the principles of building complex information protection systems, research and use of modern procedures for providing basic information security services in banking systems, which are based on the use of symmetric and asymmetric cryptography algorithms in communication systems, public key infrastructure (PCI) protocols

Structural and logical scheme of the course

Prerequisites	Postrequisites
Architecture of Computers and Computer Networks	Complex training
Databases	Pre-diploma practice
Programming the Internet	Diploma project
Software quality and testing	

Course content

Module 1. *Application and Data Security Fundamentals*

Topic 1. Basic concepts and definitions of cyber security

Topic 2. Fundamentals of cryptography. Simple encryption algorithms

Topic 3. Authentication protocols. Digital signature.

Topic 4. PGP system.

Module 2. *Security Tools*

Topic 5. Algorithms for ensuring data integrity

Topic 6. Ensuring data security at the network level

Teaching environment (software)

Internet, PNS of S. Kuznets HNUE, ZOOM

Assessment system

The system of assessment of the formed competencies takes into account the types of classes, which include lectures, laboratory classes, as well as independent work. The assessment of students' competencies is based on a cumulative 100-point system. Current control, which is carried out during the semester during practical (seminar) classes and independent work, is assessed by the sum of the points scored. The maximum possible number of points for current and final control during the semester is 100 and the minimum possible number of points is 60.

The current control includes the following control measures: assignments on topics; current control works; presentations on topics and writing essays.

More detailed information on the assessment and accumulation of points in the discipline is provided in the work plan (technological map) for the discipline.

Course policies

The teaching of the discipline is based on the principles of academic integrity. Violations of academic integrity include academic plagiarism, fabrication, falsification, cheating, deception, bribery, and biased assessment. For violations of academic integrity, students are held to the following academic responsibility: re-assessment of the relevant type of academic work.

More detailed information on competencies, learning outcomes, teaching methods, forms and methods of assessment, and independent work is provided in the Work Program of the discipline.