МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи
____
Каріна НЕМАШКАЛО

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

робоча програма навчальної дисципліни

Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітній рівень	*перший (бакалаврський)*
Освітня програма	*Інженерія програмного забезпечення*

Статус дисципліни	**обов’язкова**
Мова викладання, навчання та оцінювання	**англійська**

Завідувач кафедри
кібербезпеки та інформаційних технологій *Сергій Євсеєв*

Харків
2021

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS

"APPROVED"
Vice-rector for educational and methodical work
_______________________ Karina NEMASHKALO

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№0207121

PROGRAM AND DATA SECURITY

working program of the discipline

Branch of knowledge	*12 Information technologies*
Specialty	*121 Software Engineering*
Educational level	*first (bachelor's)*
Educational program	*Software engineering*

Discipline status	*basic*
Language of instruction, teaching and assessment	*English*

Head of Department
cybersecurity and
information technology _____________ *Serhii YEVSEIEV*

Kharkiv
2021

APPROVED
at a meeting of the Department of Cybersecurity and Information Technology
Protocol № 1 dated 27.08. 2021

Developers:
Stanislav MILEVSKYI, Ph.D., Assoc. Department of KIT.

Update and re-approval letter
working program of the discipline

Academic year	Date of the meeting of the department-developer of RPND	Protocol number	Signature of the head of the department

Abstract of the discipline

The thematic plan of the discipline and its content by modules and topics, plans of lectures and laboratory classes, material on consolidation of knowledge (tasks for independent work, control questions), methodical recommendations and assessment of students' knowledge are given. The revolutionary changes of the last decade, which took place in Internet resources, led to the unification of information and computer networks into a single information and cyberspace, which led to the creation of information and corporate networks based on Internet technologies, which significantly expanded the range of electronic services. society as a whole and man individually. As a result, threats to such an information resource as the Internet resource (IP) have also been significantly transformed. Threats to IP security have become signs of hybridity.

The spread of Internet technologies also undoubtedly requires well-placed protection of information circulating in cyberspace. Therefore, the study of the basic mechanisms of security, software protection throughout the cycle of its existence is given much attention.

The aim is to teach students the principles of software protection throughout its existence, research and use of modern procedures for providing basic information security services in information and communication resources of Internet technologies and cyberspace, based on symmetric and asymmetric cryptography algorithms, digital signatures and infrastructure protocols. public keys (IPC).

The results of the discipline are the acquisition of practical skills to determine the level of security of program code, formed using different programming languages and the use of the latest ways to protect information content in the deployment and operation of applications.

Characteristics of the discipline

Course	**4**
Semester	**7**
Number of ECTS credits	**4**
Form of final control	**Credit test**

Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Discrete Math	Software engineering
Computer systems and computer architecture	Internet programming
Computer networks	Software architecture and design

Competences and learning outcomes in the discipline

Competences	Learning outcomes
PC02. Ability to apply knowledge in practical situations. PC06. Ability to analyze, select and apply methods and tools to ensure information security (including cybersecurity). PC07. Possession of knowledge about information data models, ability create software for data storage, extraction and processing. PC10. Ability to accumulate, process and systematize professional knowledge on software creation and maintenance and recognition of the importance of lifelong learning	LO21. Know, analyze, select, qualified to apply information security (including cybersecurity) and data integrity in accordance with the applied tasks and software systems.

Curriculum

Content module 1. Data security and protection

Topic 1.*Mechanisms and policies for the distribution of access rights*
Topic 2. *Encryption mechanisms. Symmetric and asymmetric cryptosystems*
Topic 3. Authentication protocols. Digital signatures
Topic 4. Integrated data protection systems
Topic 5.*The main types of software attacks. Fundamentals of cryptanalysis*
Topic 6.*Fundamentals of digital steganography*

Content module 2. Security in software

Topic 7. *Fundamentals of Public Key Technology (PKI)*
Topic 8. *Software protection in Internet technologies*
Topic 9. *Protection of personal data*
Topic 10. *Basic principles of software protection*

The list of laboratory classes, as well as questions and tasks for independent work is given in the table "Rating-plan of the discipline".

Teaching and learning methods

In the course of teaching the discipline the teacher uses explanatory-illustrative (information-receptive) and reproductive teaching methods. Lectures (1-10), presentations (1-10) are used as teaching methods that are aimed at activating and stimulating the educational and cognitive activities of applicants.

The procedure for evaluating learning outcomes

The system of assessment of formed competencies in students takes into account the types of classes, which according to the curriculum of the discipline include lectures and laboratory classes, as well as independent work. Assessment of the formed competencies of students is carried out according to the accumulative 100-point system. Control measures include:

1) current control, which is carried out during the semester during lectures and laboratory classes and is estimated by the amount of points scored (maximum amount - 100 points; the minimum amount that allows a student to set off - 60 points);

2) final / semester control, which is conducted in the form of a test, in accordance with the schedule of the educational process.

The procedure for the current assessment of students' knowledge.

Assessment of student knowledge during lectures and laboratory classes is carried out according to the following criteria:

- analyze the crypto-resistance of simple symmetric ciphers;
- apply modern symmetric block ciphers and encryption modes;
- to study modern asymmetric cryptosystems of encryption;
- investigate electronic digital signature;
- apply steganographic methods of information protection;
- analyze the security of personal confidential data based on a secret disk and secure PGP e-mail;
- to conduct statistical studies of generators of random and pseudo-random sequences according to the NIST method.

The discipline provides the following methods of current formative assessment: questioning and oral comments of the teacher on his results, instructions of teachers in the process of laboratory tasks, the formation of self-assessment skills and discussion of students completed laboratory tasks, control of independent performance of an individual task.

All work must be done independently in order to develop a creative approach to solving problems.

Lectures: the maximum number of points is 36 (work on lectures - 12, express survey - 24).

Laboratory occupation: the maximum number of points is 64 (defense of laboratory works - 40, control works - 24), and the minimum - 50.

Individual work:consists of the time that the applicant spends on preparation for laboratory work and on preparation for express surveys of lectures and tests for laboratory work of the discipline, in the technological map points for this type of work are not allocated.

Final control:is based on the scores obtained during the semester.

A student should be considered certified if the sum of points obtained from the results of the final / semester performance test is equal to or exceeds 60.

The final grade in the discipline is calculated taking into account the points obtained during the current control of the accumulative system. The total result in points for the semester is: "60 or more points - credited", "59 or less points - not credited" and is entered in the test "Statement of performance" of the discipline.

The final grade is set according to the scale given in the table "Grade scale: national and ECTS".

Forms of assessment and distribution of points are given in the table "Rating-plan of the discipline".

Assessment scale: national and ECTS

The sum of points for all types of educational activities	Rating ECTS	Score on a national scale	
		for exam, course project (work), practice	for offset
90 - 100	AND	perfectly	credited
82 - 89	B	fine	
74 - 81	C		
64 - 73	D	satisfactorily	
60 - 63	E		
35 - 59	FX	unsatisfactorily	not credited

Rating plan of the discipline

Topic	**Forms and types of education**		**Forms of evaluation**	**Max ball**
Topic 1	***Classroom work***			
	Lecture	Lecture *"Mechanisms and policies for the distribution of access rights"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №1. Classic symmetrical systems. Investigation of cryptoresistance of simple symmetric ciphers*	performing laboratory work	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 2	***Classroom work***			
	Lecture	Lecture *"Encryption mechanisms. Symmetric and asymmetric cryptosystems"*	Work on lectures	1
			Express survey	3
	Laboratory lesson	*Laboratory work №1. Classic symmetrical systems. Investigation of*	Protection of laboratory	5

		cryptoresistance of simple symmetric ciphers	works № 1	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 3	***Classroom work***			
	Lecture	Lecture *"Authentication protocols. Digital signatures"*	Work on lectures	2
			Express survey	3
	Laboratory lesson	Laboratory work № 2. Research of modern block symmetric ciphers and encryption modes	Protection of laboratory works № 2	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 4	***Classroom work***			
	Lecture	Lecture *"Integrated data protection systems"*	Work on lectures	1
	Laboratory lesson	Laboratory work №3. Research of modern asymmetric cryptosystems of encryption. Standard DSTU ISO \ IEC 15948-2	performing laboratory work	
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 5	***Classroom work***			
	Lecture	Lecture*"Basic types of software attacks. Fundamentals of cryptanalysis"*	Work on lectures	2
			Express survey	3
	Laboratory lesson	Laboratory work №3. Research of modern asymmetric cryptosystems of encryption. Standard DSTU ISO \ IEC 15948-2 Laboratory work № 4. Research of electronic digital signature. El Gamal CPU, DSTU 4145, ECDSA	Protection of laboratory works № 3	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		

Topic 6	***Classroom work***			
	Lecture	Lecture *"Fundamentals of digital steganography"*	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 4. Research of electronic digital signature. El Gamal CPU, DSTU 4145, ECDSA	Protection of laboratory work № 4	5
			Test work 1	12
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 7	***Classroom work***			
	Lecture	Lecture *"Fundamentals of Public Key Technology (PKI)"*	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 5. Security of personal confidential data based on secret disk and secure PGP e-mail	Protection of laboratory work № 5	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 8	***Classroom work***			
	Lecture	Lecture *"Software protection in Internet technologies"*	Work on lectures	1
	Laboratory lesson	Laboratory work № 6. Steganographic methods of information protection	Express survey	3
			Protection of laboratory work № 6	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 9	***Classroom work***			
	Lecture	Lecture *"Protection of personal data"*	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 7. Statistical studies of pseudo-random, random and sequence generators according to the NIS method	Protection of laboratory work № 7	5
			Test work № 2	12
	Individual work			

	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 10	***Classroom work***			
	Lecture	Lecture *"Basic principles of software protection"*	Work on lectures	1
			Express survey	3
	Laboratory lesson	Laboratory work № 8. Deployment and management of public key infrastructure	Protection of laboratory work № 8	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		

Recommended Books

Basic

1. Information protection technologies. Multimedia interactive electronic edition of combined use / style. Evseev SP, King OG, Ostapov SE, Kots GP - Kh .: KhNEU them. S. Kuznets, 2016. - 1013 Mb. ISBN 978-966-676-624-6

2. Techniques for Designing and Analyzing Algorithms By Douglas R. Stinson Published August 6, 2021 by Chapman and Hall/CRC 444 Pages

3. Information Security Management Systems A Novel Framework and Software as a Tool for Compliance with Information Security Standard By Heru Susanto, Mohammad Nabil Almunawar 2021 by Apple Academic Press 326 Pages

Optional

4. Information Security and Optimization Edited By Rohit Tanwar, Tanupriya Choudhury, Mazdak Zamani, Sunil Gupta 2021 by Chapman and Hall/CRC 224 Pages

5 Cybercrime and Information Technology The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices By Alex Alexandrou 2021 by CRC Press 454 Pages

Information resources.

6. Site of personal educational systems of KhNEU named after S. Kuznets in the discipline "Security of programs and data" https://pns.hneu.edu.ua/enrol/index.php?id=8115.