

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
ODESSA I.I. Mechnikov NATIONAL UNIVERSITY
Department of mathematical support of computer systems



Vice-rector for scientific and pedagogical work

20__

WORKING PROGRAM OF EDUCATIONAL COURSE

OK6 “Design of complex information protection systems”

(course name)

Level of higher education Second (master's)

Field of knowledge 12 – Information technologies

Specialty 126 – Information systems and technologies
(code and name of specialty)

Educational and professional program Information systems and technologies
(EPP/ESP name)

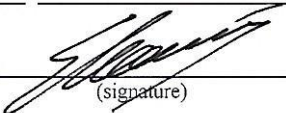
Working program of the study course "Design of complex information protection systems". – Odesa: ONU, 2022. – 10 p.

Developers:


I.M. Shpinareva, PhD (Physics and Mathematics), Associate Professor of the Department of MSCS

The work program was approved at the meeting of the Department of Mathematical Support of Computer Systems

Protocol No. 1 from " 25 " 08 2022 year

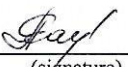
Head of the department  (Eugene MALAKHOV)
(signature) (First Name Surname)

Agreed with the guarantor of the EPP "Information systems and technologies"

 (Eugene MALAKHOV)
(signature) (First Name Surname)

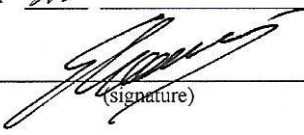
Approved by the educational and methodical commission (EMC) for IT specialties of the FMPhIT

Protocol No. 1 from " 31 " 08 2022 year

Head of EMC  (Alla RACHYNSKA)
(signature) (First Name Surname)

Reviewed and approved at the meeting of the department _____

Protocol No. 1 from " 29 " 08 2023 year

Head of Department  (_____)
(signature) (First Name Surname)

Reviewed and approved at the meeting of the department _____

Protocol No. ____ from " ____ " _____ 20 ____ year

Head of Department _____ (_____)
(signature) (First Name Surname)

1. Course description

Name of indicators	Field of knowledge, specialty, specialization, level of higher education	Characteristics of the academic discipline	
		<i>full-time education</i>	<i>external form of education</i>
Total number: credits – 3.5 hours - 105 content modules – 2	Branch of knowledge <u>12 - Information technologies</u> Specialty <u>126 -Information systems and technologies</u> Level of higher education: Second (master's)	<i>Mandatory</i>	
		<i>Year of preparation:</i>	
		2nd	
		<i>Semester</i>	
		3rd	
		<i>Lectures</i>	
		16 hours	8 hours
		<i>Practical, seminar</i>	
		<i>Laboratory</i>	
		16 hours	6 hours
		<i>Independent work</i>	
		73 hours	91 hours
		Final control form: exam	

* - in the presence

2. The purpose of discipline

The discipline is intended for the formation of knowledge about the main methods of organizing a complex information protection system.

The goal is to train future specialists in the skills and competencies to ensure an effective comprehensive system of information protection, necessary for further work, and to teach them how to apply methods and means of protection in the conditions of widespread use of modern information technologies.

The main tasks of the discipline are:

- familiarization with the methods and means of the integrated information protection system (IIPS), with the principles of organization and stages of the development of the IPS;
- study of cryptographic protocols for information protection;
- study of software and hardware means of information protection in computer networks;
- preparation for the implementation of diploma projects, the subject of which is related to information security.

The process of studying the discipline is aimed at forming elements of the following **competencies**:

SC01. The ability to develop and apply ICT (Information and Communication Technology) necessary for solving strategic and current tasks.

SC03. The ability to design information systems considering their purpose, incomplete or insufficient information, and conflicting requirements.

SC06. The ability to manage information risks based on the concept of information security.

SCM06. The ability to provide the analysis, implementation, and support of complex information security systems (combinations of regulatory, organizational, technical means and methods, procedures, practical techniques, etc.).

Program learning outcomes:

LO03. Make effective decisions on the development of information infrastructure, creation, and application of ICT.

LO10. Ensure quality cybersecurity for ICT, plan, organize, implement, and monitor the functioning of information security systems.

Expected learning outcomes. As a result of studying the academic discipline, the student should

know: the main theoretical provisions of CIPS, methods of designing complex information protection systems using modern hardware and software tools and protection methods.

be able: determine the main threats to information protection systems, personnel, and information resources and formulate requirements for protection against these threats, apply protection mechanisms that are implemented in software and hardware complexes, with the aim of building CIPS.

3. Course content

Content module 1. Stages of designing CIPS

- Topic 1.** Concept of CIPS, purpose and functions. Principles of building a comprehensive information protection system. The goals of the system approach to information protection. Information protection strategies.
Literature: [1, 2, 3, 5, 8, 9].
- Topic 2.** Formation of general requirements for CIPS.
Literature: [1, 2, 3, 4, 5, 6].
- Topic 3.** Justification of the need to create CIPS.
Literature: [1, 5, 6, 7, 9].
- Topic 4.** Inspection of operating environments.
Literature: [4, 5, 6, 8, 9].
- Topic 5.** Formulation of the task to create CIPS. Basic requirements for a comprehensive information protection system
Literature: [1-9].
- Topic 6.** Development of information security policy.
Literature: [5-9].

Content module 2. Organizational activities and support of CIPS

- Topic 7.** Development of the technical task for the creation of CIPS.
Literature: [6, 7, 8, 9].
- Topic 8.** Development of the CIPS project. The main stages of designing CIPS. Factors affecting the selection of the composition of the CIPS. A model of the automated information protection design system
Literature: [5, 8, 9, 10].
- Topic 9.** Implementation of CIPS and assessment of information security. Support of CIPS.
Literature: [7, 8, 9, 10].

4. Course structure

Names of topics	Number of hours									
	Full-time					Correspondence form				
	That's all	including				That's all	including			
		1	p/s	lab	Wed		1	p/s	lab	Wed
1	2	3	4	5	6	7	8	9	10	11
Content module 1. Stages of designing CIPS										
Topic 1. Concept of CIPS, purpose and functions. Principles of building a comprehensive information protection system.	9	1			8	5	0.5			5

Topic 2. Formation of general requirements for CIPS	11	1		2	8	5	0.5			5
Topic 3. Justification of the need to create CIPS	12	2		2	8	11	1		1	10
Topic 4. Examination of operating environments	12	2		2	8	10	1			10
Topic 5. Formulation of the task to create CIPS.	12	2		2	8	12	1		1	10
Topic 6. Development of information security policy	12	2		2	8	12	1		1	10
Together according to content module 1	68	10		10	48	55	5		3	50
Content module 2. Organizational activities and support of CIPS										
Topic 7. Development of the technical task for the creation of CIPS	12	2		2	8	16	1		1	13
Topic 8. Development of the CIPS project. The main stages of designing CIPS.	12	2		2	8	17	1		1	14
Topic 9. Implementation of CIPS and assessment of information security. Support of CIPS.	13	2		2	9	17	1		1	15
Together according to content module 3	37	6		6	25	50	3		3	41
Only hours	105	16		16	73	105	8		6	91

5. Topics of seminar classes

Seminar classes are not provided.

6. Topics of practical classes

Practical classes are not provided.

7. Topics of laboratory classes

No s/p	Topic name	Number hours
1	Basic skills of working with the Packet Tracer program. Setting up network services. DHCP, WEB, FTP server	1
2	NAT service.	1
3	ACL access control lists	2
4	Cisco ASA 5505. FirewallAppliance.	2
5	Construction of a demilitarized zone	2
6	Building VPN in Packet Tracer.	2
7	Building VPN with help CiscoASA.	2
8	AAA protocol	2

9	WI-FI network protection.	2
	Together	16

8. Independent work

No s/p	Topic name	Number hours
1	Concept of CIPS, purpose and functions. Analysis of the main functions of CIPS [1].	3
2	Analysis and assessment of threats to information security. Analysis of network security using the Wireshark sniffer [1].	7
3	Analysis of the problems caused by the creation of CIPS. Security analysis technology. Mechanisms of operation of security scanners: scanning and probing. Scheme of security analysis (Internet Scanner systems) [1]	7
4	Justification of the need to create CIPS. Analysis of the problems caused by the creation of CIPS [1].	7
5	Examination of operating environments. Definition of the task of protection and model of the violator [1]	7
6	Development of information security policy [1].	7
7	Development of the technical task for the creation of CIPS [1].	7
8	Development of the CIPS project. Determination of the functions of CIPS according to previous technical decisions [1].	7
9	Attack detection systems. (IDS). Methods of network information analysis. Classification of IDS attack detection systems: by response method, by attack detection method (abuse detection and anomaly detection), by attack information collection method (network-based, host-based, application-level) (application-based). Components and architecture of IDS.PZ SNORT [1].	7
10	Access list development [1]	7
11	Implementation of CIPS and assessment of information security. Accompaniment of CIPS [1].	7
	Together	73

Independent work includes:

[1] – preparation for lectures, practical, seminar, laboratory classes.

9. Teaching methods

Lectures using multimedia presentation material.

10. Control methods

During the current control, an oral survey or controlled written work is carried out.

The form of final control is an exam.

During the final control, the student must answer 2 questions of the examiner from the list given in point 11.

Evaluation criteria for the final modular control:

1. The answer should be complete and short. It should not contain material that does not relate to the essence of the question.
2. Clearly formulate statements, skillfully apply the necessary formulas and knowledge of the main issues of the program.
3. Answers with false statements are evaluated based on the closeness of the answer to the correct one.
4. Omissions in the justification of statements are taken into account and this leads to a decrease in the number of points.
5. Small flaws, inaccuracies in the presentation of the material, reduce the number of points.
6. Ignorance and misunderstanding of the main idea of a theoretical question or problem leads to the withdrawal of up to 90% of points.
7. If there is no answer to the question, zero points are assigned.

11. Questions for final control

1. Explain the general concepts of information protection.
2. Define the concept of a complex system of information protection
3. Describe the principles of building a complex information protection system
4. Describe threats to information security.
5. How is information shared by access mode?
6. What secrecy vultures can be given to information and what are their validity periods?
7. What information is not a state secret?
8. What are the main measures for organizing the creation of the CIPS?
9. What is the procedure for carrying out an inspection at the object of information activity?
10. What sections and subdivisions are part of the technical task for creating the CIPS?
11. What are the requirements and functions for antivirus protection?
12. What is the purpose and procedure of inspection and certification of production?
13. What measures is organized and carried out by the executor of the work on the creation of CIPS?
14. What sections does the technical task for creating CIPS contain?
15. What is the procedure for the development and execution of the technical task for the creation of CIPS?
16. What is the purpose and procedure for monitoring the state of technical information protection?
17. Describe all possible NAT service schemes.
18. Explain which private IP addresses are used by the NAT service in each address class.
19. List the advantages and disadvantages of the NAT service.
20. List the steps for setting up a NAT service.

21. Describe the main problems in the operation of the NAT server
22. Describe what parameters control extended access lists?
23. Describe the main types of access lists.
24. Describe the functions of Firewall.
25. Peculiarities of ME Firewall functioning at different levels of the OSI model.
26. Name the main connection schemes of inter-network screens. Describe the operation of a scheme with a closed protected subnet and an open subnet that is not protected.
27. Explain the concept of an attack detection system.
28. Describe attack detection methods.
29. Explain the concept of Virtual Private Network.

12. Distribution of points received by students

Current testing and independent work									Final control (exam)	Total points
Content module #1						Content module No. 2				
T1	T2	T3	T4	T5	T6	T7	T8	T9	40	100
4	7	7	7	7	7	7	7	7		

T1, T2 ... - topics of content modules

Evaluation scale: national and ECTS

Total points	ECTS assessment	National scale	
90 — 100	A - "excellent"	5 "excellent"	"test"
85 - 89	B - "very good"	4 "good"	
75 - 84	C - "good"		
70 - 74	D - "satisfactory"	3 "satisfactory"	
60 - 69	E - "permissible"		
35 — 59	F - "unsatisfactory with the possibility of reassembly"	2 "unsatisfactory"	"uncounta"
0 — 34	FX – "unsatisfactory with mandatory repeat course"		

13. Educational and methodical support

Synopsis of lectures in electronic form; methodical instructions for performing laboratory work; regulations; presentation materials.

14. Recommended Books

Basic

1. Law of Ukraine "On the Protection of Information in Information and Telecommunication Systems" [Electronic resource] / Base of legislation of Ukraine // No. 80/94-BP - Access mode: <http://zakon4.rada.gov.ua/laws/show/80>

2. The complex of means of protection against NSD in AS class 1 "Rubizh-RSO" version 2 [Electronic resource] / LLC "Technical protection of information" // 2013 - Access mode: <http://tzi.com.ua/rubzh-rso-versya-20.html>
3. ND TZI 1.6-004-2013 Protection of information on objects of information activity. Provisions on the categorization of objects where information with limited access, which constitutes a state secret, circulates.
4. ND TZI 1.6-005-2013 Protection of information at objects of information activity. Regulations on the categorization of objects where information with limited access, which does not constitute a state secret, circulates.
5. Design of complex information protection systems / Textbook / V. O. Khoroshko, I. M. Pavlov, Yu. Ya. Bobalo, V. B. Dudykevich, I. R. Opirskyi, L. T. Parkhuts. Lviv: Lviv Polytechnic Publishing House, 2020. 320 c.
6. Complex systems of information protection: study guide / Yaremchuk Y. E., Pavlovsky P. V., Kataev V. S., Sinyugin V. V.] – Vinnytsia: VNTU, 2018. – 118 p.
7. Cyber security: modern protection technologies. Study guide for students of higher educational institutions. / S.E. Ostapov, S.P. Yevseev, O.G. King. – Lviv: "New World-2000", 2020. - 678 p.

Auxiliary

8. Information protection in computer systems and networks: training. manual / S.G. Semenov, A.O. Podorozhnyak, O.I. Balenko, S.Yu. Havrylenko - Kh.: NTU "KhPI", 2014. - 251 p.
9. Complex information protection systems: design, implementation, support. Collection of lectures [Electronic resource] / Grebennikov V.V. // 2015 - Access mode: http://www.cryptohistory.ru/for_students/03-KSZ
10. Buryachok V. L. Information and cyberspace: security problems, methods and means of combating it: a guide / V. L. Buryachok, S. V. Tolyupa, V. V. Semko and others. - K.: DUT-KNU, 2016. - 178 p.

15. Electronic information resources

1. Course of the Cisco Network Academy Cisco - CyberOps [Electronic resource] Access mode: www.netacad.com