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

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

ВСТУП ДО ФАХУ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

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 ECONOMIC

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
№02071211

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

INTRODUCTION TO SPECIALTY

working program of the discipline

Branch of knowledge	***12 Information technologies***
Specialty	***125 Cybersecurity***
Educational level	***first (bachelor's))***
Educational program	***Cybersecurity***

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:
Yevseiev S.P., Doctor of Technical Sciences, Full Professor, Head of CIT Department
Kovalenko S.M., Ph.D., Assoc. Prof. of the Department of CIT Department

Update and re-approval letter
working program of the discipline

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

Abstract of the discipline

Cybersecurity is a debatable area of activity. Some sources narrow its scope, arguing that it is in fact only part of information security, which applies only to the environment of computer networks (sometimes even mention only the Internet). And others, on the contrary, expand the subject of cybersecurity, and have reason to do this - because cyberspace covers computer networks, and all devices that work in these networks and all computer technology, and people who use these technologies and devices.

The goal is to achieve fundamental thinking about the essence of the specialty, rules and principles of work in the information environment of free economic science, computer architecture, principles of algorithmization and programming in C when solving problems of professional activity.

Characteristics of the discipline

Course	**1**
Semester	**1**
Number of ECTS credits	**6**
Form of final control	test

Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Computer science according to the school program	Object-oriented programming
Mathematics according to the school program	Development and analysis of algorithms

Competences and learning outcomes in the discipline

Competences	Learning outcomes
GC 1. Ability to apply knowledge in practical situations. GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 3. Ability to communicate professionally in state and foreign languages both orally and in writing.	LO 1 – apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication
GC 1. Ability to apply knowledge in practical situations GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 4. Ability to identify, pose and solve problems in a professional direction. GC 5. Ability to search, process and analyze information.	LO 2 – organize self-professional activity, choose optimum methods and ways of the decision of difficult specialized problems and practical problems in professional activity, estimate their efficiency
GC 1. Ability to apply knowledge in practical situations GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 4. Ability to identify, pose and solve problems in a professional direction. GC 5. Ability to search, process and analyze information.	LO 3 – use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity
GC 1. Ability to apply knowledge in practical situations. GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 4. Ability to identify, pose and solve problems in a professional direction. GC 5. Ability to search, process and analyze information.	LO 4 – analyze, argue, make decisions in solving complex specialized problems and practical problems in professional

	activities, which are characterized by complexity and incomplete definition of conditions, be responsible for decisions
GC 2. Knowledge and understanding of the subject area and understanding of the profession GC 4. Ability to identify, pose and solve problems in a professional direction. GC 5. Ability to search, process and analyze information.	LO 5 – adapt in the conditions of frequent change of technologies of professional activity, to predict the final result
GC 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 6 – critically comprehend the basic theories, principles, methods and concepts in teaching and professional activities
GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 4. Ability to identify, pose and solve problems in a professional direction. PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity.	LO 7 – act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international in the field of information and / or cybersecurity
GC 2. Knowledge and understanding of the subject area and understanding of the profession. GC 4. Ability to identify, pose and solve problems in a professional direction. PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity.	LO 8 – prepare proposals for regulations on information and / or cybersecurity
GC 5. Ability to search, process and analyze information. PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 7. Ability to implement and ensure the functioning of complex information security systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.). PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 9 – implement processes based on national and international standards, detection, identification, analysis and response to information and/or cybersecurity incidents
GC 2. Knowledge and understanding of the subject area and understanding of the profession. PC 2. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity. PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies.	LO 17 – provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge, concerning structural (structural-

PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 6. Ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity.	logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information streams, processes for internal and remote components
GC 1. Ability to apply knowledge in practical situations PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity.	LO 24 – solve problems of access control to information resources and processes in information and information-telecommunication (automated) systems on the basis of access control models (mandated, discretionary, role)
GC 1. Ability to apply knowledge in practical situations PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 6. Ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins.	LO 27 – solve problems of data flow protection in information, information and telecommunication (automated) systems
PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 29 – evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of means of protection in the conditions of realization of threats of different classes
PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity.	LO 32 – solve problems of management of processes of restoration of regular functioning of information and telecommunication systems with use of procedures of redundancy according to the established security policy
PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies.	LO 33 – solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory

PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	
PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 34 – participate in the development and implementation of information security and/or cybersecurity strategies in accordance with the goals and objectives of the organization
GC 1. Ability to apply knowledge in practical situations PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 7. Ability to implement and ensure the functioning of complex information security systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.). PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 35 – solve problems of providing and support of complex systems of protection of the information, and also counteraction to unauthorized access to information resources and processes in information and information and telecommunication (automated) systems according to the established policy of information and/or cybersecurity
PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 42 – implement processes for detection, identification, analysis and response to information and/or cybersecurity incidents
GC 2. Knowledge and understanding of the subject area and understanding of the profession. PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity.	LO 43 – apply national and international regulations in the field of information security and/or cybersecurity to investigate

PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	incidents
PC 1. Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards for the purpose of carrying out professional activities in the field of information and/or cybersecurity. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity.	LO 44 – solve problems of ensuring the continuity of business processes of the organization on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards
PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 45 – apply different classes of information security and / or cybersecurity policies based on risk-oriented control of access to information assets
PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 8. Ability to carry out incident management procedures, conduct investigations, assess them. PC 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	LO 46 – analyze and minimize the risks of information processing in information and telecommunications systems
GC 1. Ability to apply knowledge in practical situations GC 4. Ability to identify, pose and solve problems in a professional direction. PC 2. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity. PC 3. Ability to use software and software-hardware complexes of information protection means in information-telecommunication (automated) systems. PC 4. Ability to ensure business continuity in accordance with established information and/or cybersecurity policies. PC 5. Ability to provide protection of information processed in information and telecommunication (automated) systems in order to implement the established policy of information and / or cybersecurity. PC 6. Ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats,	LO 53 – solve the problems of analysis of program code for the presence of possible threats

cyberattacks, failures and failures of various classes and origins. PC 8. Ability to carry out incident management procedures, conduct investigations, to assess them. PC 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cybersecurity. PC 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with established information and/or cybersecurity policies.	
GC 1. Ability to apply knowledge in practical situations GC 2. Knowledge and understanding of the subject area and understanding of the profession GC 6. The ability to exercise their rights and responsibilities as a member of society, to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine. GC 7. Ability to preserve and multiply moral, cultural, scientific values and achievements of society based on understanding the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, techniques and technologies. active recreation and a healthy lifestyle.	LO 54 – be aware of the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine

Curriculum

Content module 1. Cybersecurity as a computer science

Topic 1. *Cybersecurity as a component of information technology*

Topic 2. *Data storage*

Topic 3. *Data Processing*

Topic 4. *Operating systems and networks*

Topic 5. *Algorithms*

Topic 6. *Programming languages*

Topic 7. *Software development technology*

Topic 8. *Software life cycle*

Content module 2. Cybersecurity tools

Topic 9. *Data structures*

Topic 10. *File structures*

Topic 11. *Data bases*

Topic 12. *Database management systems*

Topic 13. *History of computing*

Topic 14. *Classification of computers*

Topic 15. *Computer software structure*

Topic 15 (continues). *Computer software structure*

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 (1-15), presentations (1-15), 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:

- ability to apply basic methods of analysis of the studied phenomena, processes and design solutions;
- ability to identify cyber threats;
- ability to describe different types of malware and attacks;
- ability to produce the simplest setting up protection means;
- ability to use basic programming concepts;
- ability to describe components of computer system;
- ability to create and implement algorithms;
- ability to apply theories and methods of protection to provide information security in information and telecommunications systems;
- ability to use modern soft- and hardware for information and communication technologies.

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 16.

Laboratory classes: the maximum number of points is 84 (defense of laboratory works – 64, test – 20), 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 points 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 *"Cybersecurity as a component of information technology"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №1. Basics of working with MS Word*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 2	***Classroom work***			
	Lecture	Lecture *"Data storage"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №1. (continued) Basics of working with MS Word*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 3	***Classroom work***			
	Lecture	Lecture *"Data Processing"*	Work on lectures	1
	Laboratory lesson	*Laboratory work № 2. Basic of working with MS Excel*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 4	***Classroom work***			
	Lecture	Lecture *" Operating systems and networks "*	Work on lectures	1

	Laboratory lesson	*Laboratory work № 2(continued) Basics of working with MS Excel.*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 5	***Classroom work***			
	Lecture	Lecture *"Algorithms"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №3. Basics of working with MS PowerPoint*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 6	***Classroom work***			
	Lecture	Lecture *" Programming languages"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №3. (continued) Basics of working with MS PowerPoint*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 7	***Classroom work***			
	Lecture	Lecture *"Software development technology"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №4. Fundamentals of C programming (program structure)*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 8	***Classroom work***			
	Lecture	Lecture *" Software life cycle"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №4. (continued) Basics of working with MS PowerPoint*	defence of the laboratory work	4
			test	10
	Individual work			

	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 9	***Classroom work***			
	Lecture	Lecture *"Data structures"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №5. Fundamentals of C programming (conditional statements)*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 10	***Classroom work***			
	Lecture	Lecture *"File structures"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №6. Fundamentals of C programming (switch statement)*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 11	***Classroom work***			
	Lecture	Lecture *"Data bases"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №7. Fundamentals of C programming (conditional statements)*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 12	***Classroom work***			
	Lecture	Lecture *" Database management systems "*	Work on lectures	1
	Laboratory lesson	*Laboratory work № 7 (continued). Fundamentals of C programming (loops)*	performing laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

Topic 13	***Classroom work***			
	Lecture	Lecture *"History of computing"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №7 (continued). Fundamentals of C programming (loops)*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 14	***Classroom work***			
	Lecture	Lecture *" Classification of computers"*	Work on lectures	1
	Laboratory lesson	*Laboratory work № 8. Fundamentals of C programming (1D arrays)*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 15	***Classroom work***			
	Lecture	Lecture *"Computer software structure"*	Work on lectures	1
	Laboratory lesson	*Laboratory work №9. Fundamentals of C programming (2D arrays)*	defence of the laboratory work	4
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 16	***Classroom work***			
	Lecture	Lecture *"Topic 15 (continues). Computer software structure"*	Work on lectures	1
	Laboratory lesson	*Laboratory work № 8. Fundamentals of C programming (files)*	defence of the laboratory work	4
			test	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

Recommended Books

Basic

1. Brooks C. J., Grow, C., Craig, P., & Short, D. Cybersecurity essentials. – John Wiley & Sons, 2018.

– 767 p.

2. Johnson T. A. (ed.). Cybersecurity: Protecting critical infrastructures from cyberattack and cyber warfare. – CRC Press, 2015. – 346p.
3. The C Programming Language The Ultimate Beginner’s Guide. EasyProgramming Publisher, 2016. – 151p.
4. Kalicharan N. Learn to Program with C. – Apress. 2015. – 323p.
5. Aumasson J.-P. Serious Cryptography. A Practical Introduction to Modern Encryption. No Starch Press. 2018. – 434p.
6. Seacord R.C. Effective C. An introduction to Professional C Programming. – No Starch Press, 2020. – 305p.

Optional

7. Lehto M., Neittaanmäki P. (ed.). Cyber security: Analytics, technology and automation. – Springer, 2015. – T. 78. – 258 p.
8. Hall G., Watson E. Computer Hacking, Security Testing, Penetration Testing and Basic Security. –
9. Chio C., Freeman D. Machine learning and security: Protecting systems with data and algorithms. – " O'Reilly Media, Inc.", 2018. – 385p.
10. Bowne S. Hands-On Cryptography with Python. – Packt. 2018. – 124 p.
11. Baloch R. Ethical hacking and penetration testing guide. – CRC Press, 2017. – 523 p.
12. Laurence T. Blockchain for dummies. – John Williy & Sons, 2017. – 280 p.

Information resource

1. Web-site of personal learning systems KNEU on discipline "Introduction to Specialty"- https://pns.hneu.edu.ua/course/view.php?id=8120.