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

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

Технології програмування
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 *Ольга СТАРКОВА*

Харків
2022

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

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

Programming technologies

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 the *Department of cyber security and information technologies* — *Olha STARKOVA*

Kharkiv
2022

APPROVED
at the meeting of the Department of Cybersecurity and Information Technologies
Protocol No. 1 dated August 27, 2022

Developer:
Mikhieiev I.A., Ph.D. , Associate Professor of the Department of Cybersecurity and Information Technologies.

Update and re-approval letter
working program of the discipline

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

Abstract of the study disciplines

Programming methodology is the foundation on which specific programming technologies are built, which include a set of production processes that lead to the creation of the necessary software, as well as a description of this set of processes. In programming technology, the emphasis is on the processes of developing programs (technological processes) in the order of their passage. There may be several programming technologies for one methodology.

The subject of the educational discipline is the basic concepts and methods of algorithmization and programming, the skills of writing and debugging programs in the Python language, creating data structures, mastering the methodology of software design.

The purpose of the educational discipline is to study the basic provisions of the Python programming language, students to acquire knowledge and skills in the field of algorithm development, creation, translation and debugging of application programs, the use of Python libraries and modules to create lossless support for solving problems of analysis and protection of information systems, which is necessary for professional training of bachelors in the specialty "Cybersecurity".

The results of studying the discipline are the acquisition of practical skills in the development of algorithms for solving problems according to the technical task, code in the Python programming language , in determining the structure of the software of computer information systems, using information about mathematical, technical, information support, conducting testing of software modules in the process software debugging , determining the effectiveness of algorithms and programs.

Characteristics of the academic discipline

Course	**2**
Semester	**3, 4**
Number of ECTS credits	**12**
Form final control	assignment, exam

Structural and logical scheme of studying the discipline

Prerequisites	Post-requisites
Programming basics	Fundamentals of cryptographic protection
Development and analysis of algorithms	Basics of construction and protection of modern operating systems
	Basics of construction and protection of microprocessor systems

Competencies and learning outcomes in the discipline

Competences	Learning outcomes
CG 5. Ability to search, process and analyze information. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.	LO-9 implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents .

CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 7. The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.) CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system . CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	
CS 7. The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.) CS 12. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO-12 to develop threat and offender models.
CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 7. The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.) CS 12. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO-16 to implement complex information protection systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents.
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose	LO-17 to ensure processes of protection and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic

of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	information resources with a display of relationships and information flows, processes for internal and remote components.
CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 10. Ability apply methods and means cryptographic and technical protection information on objects informative activities .	LO-20 to ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems.
CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO-23 to implement measures to counter unauthorized access to information resources and processes in information and information and telecommunication (automated) systems.
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins.	LO-27 to solve the problems of data flow protection in information, information and telecommunication (automated) systems .
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber	LO-31 to apply theories and methods of protection

security. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 10. Ability apply methods and means cryptographic and technical protection information on objects informative activities .	to ensure the safety of elements of information and telecommunication systems.
CG 1. Ability to apply knowledge in practical situations. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 7. The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.) CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system . CS 12. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO-35 to solve the tasks of providing and supporting complex information protection systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.
CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. KF 10. Ability apply methods and means cryptographic and technical protection information on objects informative activities .	LO-37 to measure the parameters of dangerous and interfering signals during the instrumental control of information protection processes and to determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information protection system .
CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various	LO-38 to interpret the results of special measurements using

classes and origins. KF 10. Ability apply methods and means cryptographic and technical protection information on objects informative activities .	technical means, monitoring the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents of the technical information protection system.
CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment., CS 10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity. CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO-48 to implement and support intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunication systems.
CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment., CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO-49 to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems .
CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment., CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO-52 to use tools for monitoring processes in information and telecommunication systems.
CG 1. Ability to apply knowledge in practical situations. CG 4. Skill identify , set and solve problems by professional direction	LO-53 to solve the problems of software

CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. CS 3. Ability to use software and software-hardware complexes of means of information protection in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the processes of functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. The ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	code analysis for the presence of possible threats.

Curriculum

Content module 1. Basics of working with Python
Topic 1. *Introduction to Python*
Topic 2. *Basics of working with Python*
Topic 3. *Lists, tuples and dictionaries*
Topic 4. *Working with strings*
Topic 5. *Working with files*
Content module 2. Features and examples of application of the object-oriented approach
Topic 6. *Object-oriented programming in Python*
Topic 7. *Basic Python modules*
Topic 8. *Basics of working with dates and times*
Content module 3. Basics of cryptography with Pyhon. Substitution ciphers
Topic 9. *Substitution ciphers*
Topic 10. *Analysis of the ROT13 encryption algorithm*
Topic 11. *Analysis of the substitution cipher*
Content module 4. Encryption and decryption of data
Topic 12. *Encryption and decryption using a substitution cipher*
Topic 13. *Grammatical analysis of ciphers*
Topic 14. *Fundamentals of cipher cryptanalysis*

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

Teaching and learning methods

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Problem-based lectures, presentations,

conversations, individual and group mini-projects are used as teaching methods aimed at activating and stimulating the educational and cognitive activity of the applicants .

Teaching the discipline involves the involvement of explanatory and illustrative , reproductive, research methods, as well as methods of problem-based learning. Thus, during lectures, the teacher provides students with a certain amount of theoretical material on the syntax of the Python programming language (Topic 1-14), with explanations in graphic form (presentation) and with the help of examples of program code (Topic 1-14). In laboratory work, applicants have the opportunity to acquire practical software development skills based on the problem formulated according to the topic of the lesson (Topic 1-14). Improvement of practical skills occurs during the performance of individual tasks and independent work (Topic 1-14).

The given training methods are aimed at forming the ability of students to develop software based on various technologies and programming paradigms.

The procedure for evaluating learning outcomes

The system for evaluating students' formed competencies takes into account the types of classes that, according to the program of the academic discipline, include lectures and laboratory classes, as well as independent work. Assessment of students' developed competencies is carried out according to a cumulative 100-point system. Control measures include:

- current control, which is carried out during the 3rd semester during lectures and laboratory work and is evaluated by the amount of points scored (the maximum amount is 100 points; the minimum amount that allows the student to pass the credit is 60 points);

- current control, which is carried out during the 4th semester during lectures and laboratory work and is evaluated by the amount of points scored (the maximum amount is 60 points; the minimum amount that allows the student to pass the credit is 36 points);

final/semester control in the 4th semester, conducted in the form of an exam, in accordance with the schedule of the educational process.Procedure for current assessment of students' knowledge.

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

- process data, present results by developing procedural programs;
- ability to analyze and use information resources for software development;
- the ability to develop an algorithm for solving a certain task;
- knowledge of the basics of the organization of the software development environment;
- knowledge of methodology and techniques for developing modern software solutions;
- know the features of modern programming languages and their scope of application;
- use development technologies in the environment of specialized web services ;
- knowledge of data structures, file structures and computer architecture;
- the ability to use knowledge about the development of simple programs;
- ability to use software development tools.

According to the discipline, the following methods of current normative assessment are provided: survey and oral comments of the teacher based on his results, instructions of teachers in the process of performing laboratory tasks, formation of self-assessment skills and discussion by students of completed laboratory tasks, control of independent performance of individual tasks.

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

Laboratory classes:

3rd semester - the maximum number of points is 100 (performance and defense of laboratory work - 50, control work - 50), and the minimum - 60;

4th semester - the maximum number of points is 60 (performance and defense of laboratory work - 30, control work - 30), and the minimum - 36.

Independent work in the 3rd and 4th semesters: consists of the time the applicant spends on preparing for laboratory work and preparing for express surveys for 7 lectures and control work

for the laboratory work of the discipline, points for this type of work are not allocated in the technology map.

Final control in the third semester: conducted taking into account the points received during the semester.

A student should be considered certified if the sum of points obtained as a result of the final/semester performance check is equal to or higher than 60.

Final control in the fourth semester: conducted taking into account the exam.

The examination ticket covers the program of the discipline and provides for determining the level of knowledge and the degree of mastery of competencies by students .

Each exam ticket consists of 3 practical situations (one stereotypical, one diagnostic and one heuristic task), which involve the solution of typical professional tasks of a specialist at the workplace and allow to diagnose the level of theoretical training of the student and the level of his competence in the academic discipline. The evaluation of each task of the examination ticket is as follows: the first task is 20 closed-form test tasks, its completion is evaluated by 20 points; the second task is devoted to the development of software code according to the task, its implementation is evaluated by 10 points; the third task is to debug the software code, its execution is evaluated by 10 points.

The result of the semester exam is evaluated in points (the maximum number is 40 points, the minimum number that is counted is 25 points) and is entered in the appropriate column of the examination "Success record information".

A student should be considered certified if the sum of the points obtained as a result of the final/semester performance check is equal to or higher than 60. The minimum possible number of points for current and module control during the semester is 35 and the minimum possible number of points obtained on the exam is 25.

The final grade for the academic discipline is calculated taking into account the points obtained during the current control of the accumulation 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 "Performance record" of the academic discipline.

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

Rating-plan of the educational discipline

3rd semester

Topic	**Forms and types of education**		**Assessment forms**	**Max score**
Topic 1	***Auditory work***			
	Lecture	Lecture *"Introduction to Python "*	Work on lectures	
	Laboratory session	Laboratory work #1. *Data Input/Output Basics*	Protection of laboratory work No. 1	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
T	***Auditory work***			

Topic 2	Lecture	Lecture *"Fundamentals of working with Python "*	Work on lectures	
	Laboratory session	Laboratory work #2. Organization of data processing	Protection of laboratory work No. 2	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 3	***Auditory work***			
	Lecture	Lecture *"Lists, tuples and dictionaries"*	Work on lectures	
	Laboratory session	Laboratory work #3. *Organization of work with cycles*	Protection of laboratory work No. 3	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 4	***Auditory work***			
	Lecture	Lecture *"Working with strings"*	Work on lectures	
	Laboratory session	Laboratory work 5. *Working with files*	Protection of laboratory work No. 4	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 5	***Auditory work***			
	Lecture	Lecture "*Working with files"*	Work on lectures	
	Laboratory session	Laboratory work 5. *Working with files*	Protection of laboratory work No. 5	5
			Control work 1	25

	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 6	***Auditory work***			
	Lecture	Lecture *"Object-oriented programming in Python"*	Work on lectures	
	Laboratory session	Laboratory work #6 Working with classes and objects	Protection of laboratory work No. 6	10
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 7	***Auditory work***			
	Lecture	Lecture "*Python Basic Modules"*	Work on lectures	
	Laboratory session	Laboratory work No. 7. *Development of a modular structure*	Protection of laboratory work No. 7	10
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 8	***Auditory work***			
	Lecture	Lecture *"Fundamentals of working with dates and times"*	Work on lectures	
	Laboratory session	Laboratory work #8. *Working with dates and times*	Protection of laboratory work No. 8	5
			Control work 1	25
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Assignment				

Rating-plan of the educational discipline

4th semester

Topic	Forms and types of education		Assessment forms	Max score
Topic 9	***Auditory work***			
	Lecture	Lecture "*Substitution Ciphers"*	Work on lectures	
	Laboratory session	Laboratory work 9. Cryptography with Python - reverse cipher, Caesar's cipher . Cracking the cipher	Protection of laboratory work No. 9	10
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 10	***Auditory work***			
	Lecture	Lecture *"Analysis of the ROT13 encryption algorithm"*	Work on lectures	
	Laboratory session	Laboratory work 11. Analysis of the encryption algorithm ROT13	Protection of laboratory work No. 10	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 11	***Auditory work***			
	Lecture	Lecture "Analysis of Substitution Cipher"	Work on lectures	
	Laboratory session	Laboratory work 11. Analysis of the substitution cipher	Protection of laboratory work No. 11	5
			Control work 3	10
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		

Topic 12	***Auditory work***			
	Lecture	Lecture "Encryption and decryption using a substitution cipher"	Work on lectures	
	Laboratory session	Laboratory work 12. Encryption and decryption using a substitution cipher	Protection of laboratory work No. 12	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 13	***Auditory work***			
	Lecture	Lecture *"Grammatic Analysis of Ciphers"*	Work on lectures	
	Laboratory session	Laboratory work 13. *Grammatical analysis of ciphers*	Protection of laboratory work No. 13	5
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Topic 14	***Auditory work***			
	Lecture	Lecture *"Fundamentals of cipher cryptanalysis"*	Work on lectures	
	Laboratory session	Laboratory work #14 *Basics of cipher cryptanalysis*	Protection of laboratory work No. 14	5
			Control work 1	15
	Individual work			
	Questions and tasks for independent processing	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Performance of laboratory tasks		
Exam				40

Recommended Books

General

1. Python tutorial [Electronic resource] / Python tutorial — Python 3.10.6 documentation . – Access mode: https://docs.python.org/uk/3.10/tutorial/index.html
2. Krenevich A.P. Python in examples and problems. Part 1. Structured programming. Study guide for the discipline "Informatics and programming" - K.: VOC "Kyiv University", 2018. - 206 p.
3. Krenevich A.P. Python in examples and problems. Part 2. Object-oriented programming. Study guide - K.: Kyiv University of Vocational Orthodox Church, 2020. - 152 p.

4. Vysotska V.A., Oborska O.V. Python : algorithmization and programming: a study guide - Lviv: "Novy Svit - 2000" Publishing House, 2021. - 514 p.

Additional

5. Kopey V.B. The Python Programming Language for Engineers and Scientists: A Study Guide. Ivano-Frankivsk : IFNTUNG, 2019. 274c.

6. Mokin , B. I. M 74 Educational a guide for students to master the methods solving functional problems analysis in the Python language. Part 1 / B. I. Mokin , V. B. Mokin , O. B. Mokin . – Vinnytsia : VNTU, 2022. – 124 p.

7. Briggs , Jason R. Python for Kids (A Fun Introduction to Programming). / translator from English Oleksandra Gordiychuk . Lviv : Old Lev Publishing House , 2019. 400 p

8. Programming problems . _ Python programming language . Educational manual [Electronic resource] / [O. V. Obvintsev , A. P. Krenevich , B. P. Dovgiy and others]. – 2022. – Mode of access to the resource:http://matfiz.univ.kiev.ua/userfiles/files/Zadachi_z_programuvannya_3.pdf.

9. Kozub G.O. Programming : method. rec. to the lab works for students special 121 – Engineering software provision " / G. O. Kozub, N. A. Semenov; Govt . app . Luhan . _ national Taras Shevchenko University " . – Starobilsk : DZ "LNU named after Taras Shevchenko", 2020. – 108 p.

Information resources

10. Site of personal educational systems of Kharkiv National University of Economics named after Semen Kuznets in the discipline "Programming Technologies" https://pns.hneu.edu.ua.