

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



Каріна ІВМАШКАЛО

**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

Сергій ЄВСЕВ

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

Academic year	Date of the meeting of the department	Protocol	Signature of the head of the department
<b><u>PROGRAMMING TECHNOLOGIES</u></b>			
<b>working program of the discipline</b>			
Field of knowledge	<i>12 Information technologies</i>		
Speciality	<i>125 CyberSecurity</i>		
Educational level	<i>first (bachelor's)</i>		
Educational program	<i>CyberSecurity</i>		

Discipline status

*basic*

Language of instruction, teaching and assessment

*English*

Head of Department

*cybersecurity and information technology*

Sergey EVSEEV

Kharkiv

2021

APPROVED

at a meeting of the Department of Cybersecurity and Information Technology  
Protocol № 1 dated 27.08.2021

Developer:

Shmatko OV, Ph.D., Assoc. Prof of CIT Department.

**Update and re-approval letter  
working program of the discipline**

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

### Abstract of the discipline

The programming methodology is the foundation on which specific programming technologies are built, which includes a set of production processes, which leads 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 program development (technological processes) in the order of their passage. There can be several programming technologies for one methodology.

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

**The purpose** of the course is to study the basics of Python programming language, students acquire knowledge and skills in algorithm development, creation, translation and debugging of applications, use of libraries and Python modules to create software to solve problems of analysis and protection of information systems. professional training of bachelors in "Cybersecurity".

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

### Characteristics of the discipline

Course	<b>2</b>
Semester	<b>3, 4</b>
Number of ECTS credits	<b>12</b>
Form of final control	<b>test, exam</b>

### Structural and logical scheme of studying the discipline

<b>Prerequisites</b>	<b>Postrequisites</b>
Basics of programming	Fundamentals of cryptographic protection
Mathematical foundations of cryptology	Fundamentals of building and protecting modern operating systems
Fundamentals of information theory	
Fundamentals of construction and operation of microprocessor systems	

### Competences and learning outcomes in the discipline

<b>Competences</b>	<b>Learning outcomes</b>
OC 1. Ability to apply knowledge in practical situations.	LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems; LO 35 - to solve problems of providing and support of complex systems of information protection, 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; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
OC 2. Knowledge and understanding	LO 17 - to provide processes of protection and functioning of information-

<b>Competences</b>	<b>Learning outcomes</b>
of the subject area and understanding of the profession	telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components.
OC 4. Ability to identify, pose and solve problems in a professional direction.	LO 53 - to solve problems of analysis of program code for the presence of possible threats
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 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 35 - to solve problems of providing and support of complex systems of information protection, 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 2. Ability to use information and communication technologies, modern methods and models of information security and / or cybersecurity.	LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 3. Ability to use software and software-hardware complexes of information security in information and telecommunication (automated) systems.	LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents; LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components; LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems; LO 35 - to solve problems of providing and support of complex systems of information protection, 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; LO 53 - to solve problems of analysis of program code for the presence of possible threats.
PC 4. Ability to ensure business continuity 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; LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network

Competences	Learning outcomes
	<p>topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems;</p> <p>LO 35 - to solve problems of providing and support of complex systems of information protection, 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;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>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.</p>	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems;</p> <p>LO 35 - to solve problems of providing and support of complex systems of information protection, 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;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>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.</p>	<p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 27 - to solve problems of data flow protection in information, information and telecommunication (automated) systems;</p> <p>LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems;</p> <p>LO 37 - to measure the parameters of dangerous and interference signals during</p>

Competences	Learning outcomes
	<p>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;</p> <p>LO 38 - interpret the results of special measurements using technical means, control the characteristics of information and telecommunications systems in accordance with the requirements of regulatory documents of the system of technical protection of information;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>PC 7. Ability to implement and ensure the functioning of complex information security systems (complexes of legal, organizational and technical means and methods, procedures, practices, etc.).</p>	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 12 - to develop models of threats and violators;</p> <p>LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents;</p> <p>LO 35 - to solve problems of providing and support of complex systems of information protection, 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.</p>
<p>PC 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.</p>	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 35 - to solve problems of providing and support of complex systems of information protection, 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;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
<p>PC 9. Ability to carry out professional activities on the basis of the implemented information and / or cybersecurity management system.</p>	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 35 - to solve problems of providing and support of complex systems of</p>

Competences	Learning outcomes
	information protection, 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 10. Ability to apply methods and means of cryptographic and technical protection of information at the objects of information activities.	<p>LO 20 - to ensure the operation of special software for the protection of information from destructive software influences, destructive codes in information and telecommunications systems;</p> <p>LO 31 - apply theories and methods of protection to ensure the security of elements of information and telecommunications systems;</p> <p>LO 37 - to measure the parameters of dangerous and interference 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;</p> <p>LO 38 - interpret the results of special measurements using technical means, control the characteristics of information and telecommunications systems in accordance with the requirements of regulatory documents of the system of technical protection of information;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems.</p>
PC 11. Ability to monitor the functioning of information, information and telecommunications (automated) systems in accordance with the established policy of information and / or cybersecurity.	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 17 - to provide processes of protection and functioning of information-telecommunication (automated) systems on the basis of practices, skills and knowledge concerning structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with reflection of interrelations and information flows, processes for internal and remote components;</p> <p>LO 23 - implement measures to combat unauthorized access to information resources and processes in information and information and telecommunications (automated) systems;</p> <p>LO 48 - implement and maintain intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunications systems;</p> <p>LO 49 - to ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems;</p> <p>LO 52 - use tools for monitoring processes in information and telecommunications systems;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>
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.	<p>LO 9 - implement processes based on national and international standards, detection, identification, analysis and response to information and / or cybersecurity incidents;</p> <p>LO 12 - to develop models of threats and violators;</p> <p>LO 16 - to implement complex information protection systems in automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory documents;</p> <p>LO 35 - to solve problems of providing and support of complex systems of information protection, 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;</p> <p>LO 53 - to solve problems of analysis of program code for the presence of possible threats.</p>



## Curriculum of the discipline

### Content of the educational discipline

#### 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 files*

*Topic 5. Working with strings*

#### Content module 2. Features and examples of object-oriented approach

*Topic 6. Basic Python modules*

*Topic 7. Object-oriented programming in Python*

*Topic 8. Basics of working with dates and times*

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 (1-8), presentations (1-8) 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

#### 3 semester

The system of assessment of the formed competencies of students takes into account the types of classes, which in accordance with 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; minimum amount that allows students to take credit - 60 points);

2) final / semester control, which is carried out in the form of control work, in accordance with the schedule of the educational process;

3) final / semester control for the fourth semester is carried out in the form of a semester exam in accordance with the schedule of the educational process.

The order of current assessment of students' knowledge.

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

- the ability to install and configure the Python ide programming environment;
- ability to write in the environment of simple and complex expressions and Python objects;
- ability to write Python control constructs;
- ability to develop programs of medium complexity;
- the ability to create and apply user functions;
- the ability to download Python modules and call the functions of this module, work with the help information of the module.

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

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

Lectures:

3 semester - the maximum number of points - 24 (work on lectures - 14, control - 10);

Laboratory classes:

3 semester - the maximum number of points - 76 (laboratory work - 56, defense of laboratory work - 20).

Independent work in the 1st semester: consists of time that the entrant spends on preparation for laboratory work and preparation for express examinations of lectures and tests for laboratory work on the subject, in the technological map points for this type of work are not allocated.

Final control in the 3 semester: is based on the scores obtained during the semester.

A student is considered certified if the sum of points obtained as a result of the final / semester performance test is equal to 100.

### **The procedure for evaluating learning outcomes 4 semester**

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;

3) final / semester control for the fourth semester is carried out in the form of a semester exam 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 install and configure the Python ide programming environment;
- the ability to write in the environment of simple and complex expressions and Python objects;
- ability to write Python control constructs;
- ability to develop programs of medium difficulty;
- ability to create and apply user functions;
- the ability to download Python modules and call the functions of this module, work with the help information of the module.

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, formation of self-assessment skills and discussion of completed laboratory tasks, control of individual performance.

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

Lectures:

4 semester - the maximum number of points is 19 (work on lectures - 9, control work - 10);

Laboratory classes:

4 semester - the maximum number of points is 41 (performance of laboratory work - 9, defense of laboratory work - 32), and the minimum - 30;

Independent work in 4 semester: consists of time that the applicant spends on preparation for laboratory work and 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 in the third semester:** is carried out taking into account 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.

**Final control in the fourth semester:** is carried out taking into account the exam.

The examination ticket covers the program of the discipline and provides for the determination of 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 solving typical professional tasks in the workplace and allow to diagnose the level of theoretical training of the student and his level of competence in the discipline. Evaluation of each task of the examination ticket is as follows: the first task is 20 test tasks of the closed form, its performance is estimated by 20 points; the second task is devoted to the development of program code for the task, its implementation is evaluated by 10 points; the third task - debugging the program code, its execution is estimated by 10 points.

The result of the semester exam is evaluated in points (maximum number - 40 points, minimum number of credits - 25 points) and is affixed in the appropriate column of the examination "Information of performance".

A student should be considered certified if the sum of points obtained from the final / semester test is equal to or exceeds 60. The minimum possible number of points for current and modular control during the semester is 35 and the minimum possible number of points scored in the exam is 25.

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 "Assessment 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	Score EKTC	Score on a national scale	
		for exam, course project (work), practice	For credit
90 – 100	A	excellent	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

3 semester

Topic	Forms and types of education		Forms of evaluation	Max points
<b>Topic 1</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Introduction to Python"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work №1. Basics of data input / output</i>	Laboratory lesson	8
	<b><i>Individual work</i></b>			
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			
<b>Topic 2</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Fundamentals of working with Python"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work №2. Organization of data processing</i>	Laboratory lesson	8
			Answer of laboratory work	4
	<b><i>Individual work</i></b>			
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			
<b>Topic 3</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Lists, tuples and dictionaries"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work №3. Organization of work with cycles</i>	Laboratory lesson	8
	<b><i>Individual work</i></b>			
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			
<b>Topic 4</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Working with files"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work 4. Organization of calculations.</i>	Laboratory lesson	8

			Answer of laboratory work	4
	<b>Individual work</b>			
	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		
<b>Topic 5</b>	<b>Classroom work</b>			
	Lecture	<i>Lecture "Working with deadlines"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work 5. Work with files</i>	Laboratory lesson	8
			Answer of laboratory work	4
			Control work	10
	<b>Individual work</b>			
	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		
<b>Topic 6</b>	<b>Classroom work</b>			
	Lecture	<i>Lecture "Basic Python modules"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work №6. Working with lists</i>	Laboratory lesson	8
			Answer of laboratory work	4
	<b>Individual work</b>			
		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	
<b>Topic 7</b>	<b>Classroom work</b>			
	Lecture	<i>Lecture "Object-Oriented Programming in Python"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work № 7. Work with two-dimensional arrays</i>	Laboratory lesson	8
			Answer of laboratory work	4
	<b>Individual work</b>			
		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	
<b>Topic 8</b>	<b>Classroom work</b>			
	Lecture	<i>Lecture "Fundamentals of working with dates and times"</i>	Lecture	
	Laboratory lesson	<i>Laboratory work 8. Work with functions</i>	Laboratory lesson	
			Answer of	

			laboratory work	
	<b><i>Individual work</i></b>			
	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		

**Rating plan of the discipline  
4 semester**

<b>Topic</b>	<b>Forms and types of education</b>		<b>Forms of evaluation</b>	<b>Max points</b>
<b>Topic 1</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Introduction to Python"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work №1. Basics of data input / output</i>	Laboratory lesson	5
	<b><i>Individual work</i></b>			
	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		
<b>Topic 2</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Fundamentals of working with Python"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work №2. Organization of data processing</i>	Laboratory lesson	1
			Answer of laboratory work	4
	<b><i>Individual work</i></b>			
	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		
<b>Topic 3</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Lists, tuples and dictionaries"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work №3. Organization of work with cycles</i>	Laboratory lesson	5
	<b><i>Individual work</i></b>			
	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		

<b>Topic 4</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Working with files"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work 4. Organization of calculations.</i>	Laboratory lesson	1
			Answer of laboratory work	4
	<b><i>Individual work</i></b>			
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			
<b>Topic 5</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Working with deadlines"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work 5. Work with files</i>	Laboratory lesson	1
			Answer of laboratory work	4
			Control work	10
<b><i>Individual work</i></b>				
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			
<b>Topic 6</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Basic Python modules"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work №6. Working with lists</i>	Laboratory lesson	1
			Answer of laboratory work	4
	<b><i>Individual work</i></b>			
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			
<b>Topic 7</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Object-Oriented Programming in Python"</i>	Lecture	1
	Laboratory lesson	<i>Laboratory work № 7. Work with two-dimensional arrays</i>	Laboratory lesson	1
			Answer of laboratory work	5
	<b><i>Individual work</i></b>			
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			

<b>Topic 8</b>	<b><i>Classroom work</i></b>			
	Lecture	<i>Lecture "Fundamentals of working with dates and times"</i>	Lecture	2
	Laboratory lesson	<i>Laboratory work 8. Work with functions</i>	Laboratory lesson	1
			Answer of laboratory work	4
	<b><i>Individual work</i></b>			
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			
<b>Final exam</b>			<b>40</b>	

### Recommended Books

#### Basic

1. Allen Mark. Python for Beginners: A Step by Step Guide on How to Program with Python. Amazon Digital Services LLC, 2019. — 97 p
2. Alvaro F. Python: Easy Python Programming For Beginners, Your Step-By-Step Guide to Learning Python Programming. New York: Felix Alvaro, 2017. — 98 p
3. Ambli Shreeharsh. Learn Python: Step-By-Step. Amazon.com Services LLC, 2020. — 40 p
4. Summerfield, M. Programming in Python 3. A detailed guide / M. Summerfield. - M.: Symbol, 2016. -- 608 p.
5. Ahidjo Ayeva, Kamon Ayeva, Aiman Saeed Python In - Depth: Use Python Programming Features, Techniques, and Modules to Solve Everyday Problems, India, New Delhi: BPB Publications, 2021.

#### Additional

6. Amos D., Bader D., Jablonski J., Heisler F. Python Basics: A Practical Introduction to Python 3. New York: Real Python, 2021. — 643 p.
7. Albee B. Hands-On Software Engineering with Python. Birmingham: Packt Publishing, 2018. — 736 p.
8. Aline Anthony. Python Programming: A Step By Step Guide From Beginner to Advanced (Beginner & Advanced). Independently published, 2020. — 173 p.
9. Allen Mark. Python for Beginners: A Step by Step Guide on How to Program with Python. Amazon Digital Services LLC, 2019. — 97 p.
10. Althoff Cory. The Self-taught Programmer: The Definitive Guide to Programming Professionally. 2016. — 256 p.

#### Information resources.

11. Site of personal educational systems of S. Kuznets KhNEU in the discipline "PROGRAMMING TECHNOLOGIES" <https://pns.hneu.edu.ua/course/view.php?id=4929>.