

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

"ЗАТВЕРДЖУЮ"

Проректор з навчально-методичної роботи
Каріна НЕМАШКАЛО



РОЗРОБКА ТА АНАЛІЗ АЛГОРИТМІВ

робоча програма навчальної дисципліни

Галузь знань	<i>12 Інформаційні технології</i>
Спеціальність	<i>125 Кібербезпека</i>
Освітній рівень	<i>перший (бакалаврський)</i>
Освітня програма	<i>Кібербезпека</i>

Статус дисципліни	<i>обов'язкова</i>
Мова викладання, навчання та оцінювання	<i>англійська</i>

Завідувач кафедри
кібербезпеки
та інформаційних технологій

Ольга СТАРКОВА

Харків
2022

ЗАТВЕРДЖЕНО

на засіданні кафедри кібербезпеки та інформаційних технологій
Протокол № 1 від 27.08.2022 р.

Розробники:

Солодовник Ганна Валеріївна, к.т.н., доцент кафедри КІТ

**Лист оновлення та перезатвердження
робочої програми навчальної дисципліни**

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

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

"APPROVED"

Vice-rector for educational and methodical work

Karina NEMASHKALO



ALGORITHM DEVELOPMENT AND ANALYSIS

working program of the educational discipline

Area of expertise	<i>12 Information technologies</i>
Speciality	<i>125 Cybersecurity</i>
Grade level	<i>First (Bachelor's level)</i>
Academic Program	<i>Cybersecurity</i>

Type of discipline	<i>basic</i>
Teaching, studying and evaluating language	<i>English</i>

Head of the *Department of cyber security
and information technologies*

Olha STARKOVA

Kharkiv
2022

APPROVED

At the session of the Cybersecurity and Information Technology Department
Protocol № 1 from 27.08. 2022.

Drafters:

*Solodovnyk Ganna, c.t.s., associate professor of Cybersecurity and Information Technology
Department*

**The list of renewal and re-approval
of academic discipline program**

Academic year	Data of the session of the Department – Drafter of SDAD	Protocol Number	Signature of Head of Department

Introduction

Annotation for the academic discipline:

The task of the discipline "Development and analysis of algorithms" is formation of skills and competence in the field of algorithm development and analysis of their complexity. Teaching of the discipline involves familiarization of the applicants with the basic concepts of algorithmization, acquisition of skills of compilation and analysis of labor-intensive algorithms of different types of computing processes, teaching of use of classical algorithms: sorting, working with data of different structures, creation and processing of trees and graphs, working with matrices and networks, greedy algorithms, etc.

The subject of the discipline is algorithms, as well as modern methods of building and analysis of algorithms with the use of effective methods of storage, representation and transformation of information.

The purpose of the academic discipline "Development and analysis of algorithms" is to form systematic knowledge about theoretical bases of algorithm development and analysis; acquire skills of using methods of formulation and solution of problems of algorithm development and analysis of their labor capacity; understanding of essence of algorithm provision of information systems; automation of decision of tasks of information security; construction and introduction of mathematical and computing models of processes of information processing, their optimization and determination of directions of improvement.

The results of the study of discipline are system knowledge and practical skills in the field of development and application of algorithmic models, methods of building algorithms of data processing, determination of complexity of algorithms, their improvement and optimization.

Description of the educational discipline

Course	1
Semester	2
Number of ECTS credits	5
Form of final control	examination

Structural-logical scheme of studying of discipline

Pre-requisites	Post-requisites
Cybersecurity introduction	Software engineering

Competence and learning outcomes in the discipline

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

<p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 7. Ability to implement and provide functioning of complex systems of information protection (complexes of normative-legal, organizational and technical means and methods, procedures, practical methods, etc.).</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	
<p>CP 7. Ability to implement and provide functioning of complex systems of information protection (complexes of normative-legal, organizational and technical means and methods, procedures, practical methods, etc.).</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 12 – to develop models of threats and violators;</p>
<p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 3. Ability to use software and software-hardware complexes of means of information protection in information-telecommunication (automated) systems.</p> <p>CP 7. Ability to implement and provide functioning of complex systems of information protection (complexes of normative-legal, organizational and technical means and methods, procedures, practical methods, etc.).</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 16 – implement complex systems of information protection in the automated systems (as) of the organization (enterprises) according to the requirements of normative-legal documents;</p>
<p>CT 2. Knowledge and understanding of the subject area and understanding of the profession.</p> <p>CP 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.</p> <p>CP 3. Ability to use software and software-hardware complexes of means of information protection in information-telecommunication (automated) systems.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 6. Ability to restore normal functioning of information, information and telecommunication systems after implementation of threats,</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</p>

<p>realization of cyber attacks, failures and failures of different classes and origin. CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them. CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p>	<p>for internal and remote components;</p>
<p>CT 1. Ability to apply knowledge in practical situations. CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy. CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity. CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system. CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p>	<p>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 (mandate, discretionary, role-based);</p>
<p>CT 1. Ability to apply knowledge in practical situations. CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy. CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity. CP 6. Ability to restore normal functioning of information, information and telecommunication systems after implementation of threats, realization of cyber attacks, failures and failures of different classes and origin.</p>	<p>LO 27 – solve the problems of data stream protection in information, information and telecommunication systems;</p>
<p>CP 3. Ability to use software and software-hardware complexes of means of information protection in information-telecommunication (automated) systems. CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy. CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity. CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them. CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system. CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 29 – to carry out an assessment of the possibility of realization of potential threats of information, processed in information and telecommunication systems and effectiveness of use of complexes of protection means in conditions of realization of threats of different classes;</p>
<p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy. CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity. CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them. CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p>	<p>LO 32 – to solve problems of management of processes of restoration of normal functioning of information and telecommunication systems using procedures of reservation according to established security policy;</p>
<p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the</p>	<p>LO 33 – to solve problems of ensuring continuity of</p>

<p>purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>business processes of the organization on the basis of the risk theory;</p>
<p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 34 – participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization;</p>
<p>CT 1. Ability to apply knowledge in practical situations.</p> <p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 3. Ability to use software and software-hardware complexes of means of information protection in information-telecommunication (automated) systems.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 7. Ability to implement and provide functioning of complex systems of information protection (complexes of normative-legal, organizational and technical means and methods, procedures, practical methods, etc.).</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 35 – to solve problems of providing and maintaining complex systems of information protection, as well as to prevent unauthorized access to information resources and processes in information and information-telecommunication (automated) systems according to established policy of information security and/or cyber security;</p>
<p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p>	<p>LO 42 – implement processes of identification,</p>

<p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>identification, analysis and response to information and/or cyber security incidents;</p>
<p>CT 2. Knowledge and understanding of the subject area and understanding of the profession.</p> <p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 43 – apply national and international regulatory acts in the field of information security and/or cyber security to the investigation of incidents;</p>
<p>CP 1. Ability to apply legislative and regulatory frameworks, as well as state and international requirements, practices and standards for the purpose of professional activities in the field of information and/or cybersecurity.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 44 – to solve problems of ensuring continuity of business processes of the organization on the basis of the theory of risks and established system of information security management according to national and international requirements and standards;</p>

<p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 45 – apply security and/or cyber security policies based on a risk-oriented control of access to information assets;</p>
<p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 9. Ability to perform professional activities on the basis of the implemented information and/or cyber security management system.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 46 – analyze and minimize the risks of information processing in information and telecommunication systems;</p>
<p>CT 1. Ability to apply knowledge in practical situations.</p> <p>SHORT CIRCUIT 4. Ability to identify, set and solve problems in a professional way.</p> <p>CP 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security.</p> <p>CP 3. Ability to use software and software-hardware complexes of means of information protection in information-telecommunication (automated) systems.</p> <p>CP 4. Ability to ensure continuity of business in accordance with established information and/or cyber security policy.</p> <p>CP 5. Ability to provide protection of information processed in information-telecommunication (automated) systems for realization of established policy of information and/or cybersecurity.</p> <p>CP 6. Ability to restore normal functioning of information, information and telecommunication systems after implementation of threats, realization of cyber attacks, failures and failures of different classes and origin.</p> <p>CP 8. Ability to conduct incident management procedures, conduct investigations, and assess them.</p> <p>CP 11. Ability to monitor the processes of information, information and telecommunication (automated) systems functioning according to the established information and/or cyber security policy.</p> <p>CP 12. Ability to analyze, identify and assess potential threats, vulnerabilities and destabilizing factors in the information space and information resources according to the information and/or cyber security policy.</p>	<p>LO 53 – solve problems of analysis of program code for possible threats.</p>

Program of discipline

Content module 1. Theoretical bases of algorithm theory

Topic 1: The concept of the algorithm

Algorithms in human life. Theory of algorithms as mathematical science. Definition of algorithm. The purpose and the tasks associated with them, which are solved in the theory of algorithms. Requirements to algorithms. The basic principles on which algorithms are built. Properties of algorithms.

Topic 2: Elementary data structures.

Application structuring and abstraction. Concept of data structures. Classification of data structures. Operations on data structures. Simple data structures. Static data structures. Semi-static data structures. Dynamic data structures.

Topic 3: Double search trees.

The concept of the tree and its elements. Basic operations with wood. Binary search trees. Binary tree structure. An algorithm for inserting an item and searching for an item in a binary tree.

Topic 4: Hash tables.

Concept of hash-table. Direct addressing. Solving collisions with chains. Analysis of hashvannya with chain. Hash functions and methods of their realization. Open address. Linear and quadratic methods of calculation of sample sequences. Double hanged. Perfect hashchya.

Topic 5: Basic algorithms on graphs.

Presentation of graphs. Algorithm of search in width and its analysis. The shortest ways. Algorithm of search in depth and its analysis. Classification of ribs. Topological sorting. Highly connected components.

Topic 6: Network flows.

Concept of the network and basic definitions. Optimal network flows. The method of placing a tag to find the maximum flow and its modification. Ford-Falkerson algorithm finding maximum flow.

Content module 2. Algorithm of solving application problems

Topic 7: Greedy algorithms.

A greedy approach, its advantages and disadvantages (the problem of coins). The rule of using a greedy approach (a task about a backpack). Application of the greedy approach in practice: Haffman algorithm, Kraskala algorithm, Prima algorithm. Dynamic programming.

Topic 8: Matrix and actions with them.

Matrices and their properties. The algorithm of the Shrelane multiplication of matrices. Algebraic systems and reproduction of Boolean matrices. Solutions of linear equations systems. Address of matrixes. Positive certain symmetric matrices.

Topic 9: Theoretical and numerical algorithms.

The largest joint polling station. Modular arithmetic. Check numbers for simplicity. Number spread on multipliers.

Topic 10: Search substrings.

Algorithm of Rabina-Karpa. Search substrings using terminal machines. The Knut-Moris-Pratt algorithm. Boyer-Moore algorithm.

Topic 11: Calculated geometry.

Section properties. The average cuts. Construction of a convex shell. Searching for a pair of nearest points.

Topic 12: Approximate algorithms.

Top coating. The task of the Commissioner. The problem about coverage by sets.

The list of laboratory lessons, as well as questions and tasks for independent work is given in

the table "Rating-plan of educational discipline".

Methods of teaching

Teaching of discipline involves the involvement of explanatory-illustrative, reproductive, research methods, as well as methods of problem education. Thus during the lecture classes the teacher gives to the participants a certain volume of theoretical material, with explanations in graphic form (schemes, tables, presentations) and with the help of examples of solution of problems. At the laboratory classes, the applicants can get practical skills in solving problems on the basis of the problem formed by the subject of the class. Improvement of practical skills takes place during individual tasks (Topics 3, 4, 5, 6) and independent work (Topics 7, 8, 9, 10, 11).

The methods of training are aimed at formation of the ability of the applicants to solve complex complex problems in the field of algorithmization.

The procedure of evaluation of the learning results

The program of the educational discipline provides lecture, laboratory and independent kinds of work. The knowledge and competence received by the participants during the lecture sessions are assessed by writing of control works and drawing up tests, the skills received during the laboratory sessions are assessed by the solving of tasks provided by the subject of work. The independent work is not evaluated separately, because it consists in preparation for other types of lessons. The assessment of the formed competencies of the applicants is carried out according to the rating accumulated 100-point system. Control measures include:

- the current control, which is carried out during the semester during the lecture and laboratory classes and is assessed by the sum of the points collected (maximum amount – 60 points; minimum amount, which gives the student to make the exam – 35 points);
- modular control provides for the fulfillment of final control tasks, which may include creative research component and require knowledge and skills obtained during the study of a certain sum of material by the subject of the module;
- the final control consists in the preparation of the semester exam for the discipline and provides written work on the subject of the whole course, the purpose of which is to determine the level of understanding of the program material by the applicant in general, the logic of relations between the sections of the course and the subject of the related disciplines.

For the current control, the knowledge of the applicants is assessed according to the following criteria:

- free possession of teaching material in full, understanding of examples and the possibility of providing own examples to explain the essence of the material;
- demonstration of skills of application of methods of building algorithms for solving application problems;
- demonstration of the skills of innovative methods of work in solving problems;
- demonstration of the ability to find and analyze sources of information, to base the results and to draw conclusions on the work;
- training of team work skills during complex tasks of algorithm development and analysis.

Task-making and control over their implementation are aimed at assisting the acquisition of skills of active creative thinking, strengthening of cognitive skills and norms of good cooperation. The main requirement for the performance of tasks is independence of their execution or determination of the percentage of the deposit on condition of teamwork.

The distribution of points of the current assessment by types of work is the following.

Lecture classes: The level of mastering by theoretical knowledge is determined during the protection of laboratory works, for writing of control works (the maximum number of points is – 18).

Laboratory lessons: The level of acquired skills of application of knowledge for solving

problems is determined by the correctness of execution of tasks of laboratory works (maximum number of points is 42).

Self-work: The level of mastering skills of using the newest knowledge, methodology and methods of conducting scientific researches is determined by the degree of preparation of the postgraduate student for execution of laboratory works and writing of control works (in the technological card of additional points on this type of works is not provided).

Final control: Is carried out taking into account the examination.

The examination ticket covers the discipline program and provides for the determination of the level of knowledge and degree of training of the applicants. Each exam ticket consists of 2 theoretical questions and 1 practical tasks, which provide solution of typical professional tasks of the specialist at the workplace and allow to diagnose the level of theoretical training of the student and the level of his competence in the educational discipline. The evaluation of each task of the examination ticket is as follows: The first theoretical question is estimated by 10 points; the second question is estimated by 10 points; the third practical task is estimated by 20 points.

The result of the semester exam is estimated in points (maximum number – 40 points, minimum number, which is counted – 25 points) and is placed in the corresponding column of the exam "Information of the record of success". The recipient should be considered attested if the sum of points received on the results of the final/semester check of success is equal to or exceeds 60. The minimum number of points for the current and modular control during the semester is 35 and the minimum number of points for the examination is 25. The final evaluation of the training discipline is calculated taking into account the points received during the examination and the points received during the current control over the accumulation system. The total result in points for the semester is: "60 and more points – scored", "59 and less points – not scored" and is entered in the "track record of success" of the educational discipline.

The assessment and allocation of points are presented in the table "Rating-plan of the educational discipline".

Rating-plan of the educational discipline

T o p i c	Forms and types of training		Evaluation forms	Max score
T o p i c 1	<i>Audience work</i>			
	Lecture	Lecture 1. The concept of the algorithm	Work at the lecture	
	Laboratory research	Laboratory work №1. Algorithm construction and analysis	Laboratory work	
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 2	<i>Audience work</i>			
	Lecture	Lecture 2. Elementary data structures	Work at the lecture	
	Laboratory research	Laboratory work №1. Algorithm construction and analysis	Execution and defense of laboratory work	7
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 3	<i>Audience work</i>			
	Lecture	Lecture 3. Double search trees	Work at the lecture	
	Laboratory research	Laboratory work №2. Programming basic data structures	Laboratory work	
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c	<i>Audience work</i>			
	Lecture	Lecture 4. Hash tables	Work at the lecture	
	Laboratory research	Laboratory work №2. Programming basic data structures	Execution and defense of	7

4			laboratory work	
		Revision of the module	Revision of the topics 1-4	9
<i>Independent study</i>				
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 5	<i>Audience work</i>			
	Lecture	Lecture 5. Basic algorithms on graphs	Work at the lecture	
	Laboratory research	Laboratory work №3. Search binary trees	Laboratory work	
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 6	<i>Audience work</i>			
	Lecture	Lecture 6. Network flows	Work at the lecture	
	Laboratory research	Laboratory work №3. Search binary trees	Execution and defense of laboratory work	7
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 7	<i>Audience work</i>			
	Lecture	Lecture 7. Greedy algorithms	Work at the lecture	
	Laboratory research	Laboratory work №4. Floyd-Warshall algorithm	Laboratory work	
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p	<i>Audience work</i>			
	Lecture	Lecture 8. Matrix and actions with them	Work at the lecture	

i c 8	Laboratory research	Laboratory work №4. Floyd-Warshall algorithm	Execution and defense of laboratory work	7
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 9	<i>Audience work</i>			
	Lecture	Lecture 9. Theoretical and numerical algorithms	Work at the lecture	
	Laboratory research	Laboratory work №5. Strassen algorithm matrix multiplication	Laboratory work	
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 1 0	<i>Audience work</i>			
	Lecture	Lecture 10. Search substrings	Work at the lecture	
	Laboratory research	Laboratory work №5. Strassen algorithm matrix multiplication	Execution and defense of laboratory work	7
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p i c 1 1	<i>Audience work</i>			
	Lecture	Lecture 11. Calculated geometry	Work at the lecture	
	Laboratory research	Laboratory work №6. Dynamic programming	Laboratory work	
		Revision of the module	Revision of the topics 1-4	9
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
T o p	<i>Audience work</i>			
	Lecture	Lecture 12. Approximate algorithms	Work at the lecture	

i c 1 2	Laboratory research	Laboratory work №6. Dynamic programming	Execution and defense of laboratory work	7
	<i>Independent study</i>			
	Questions and tasks for independent work	Search, selection and review of literature sources by a specific topic. Preparation for laboratory work. Performing laboratory tasks		
Examination				40

Recommended literature

Main

1. Tim Roughgarden Algorithms Illuminated Part 1: The Basics – Soundlikeyourself Publishing, LLC, San Francisco, CA, 2018. – 216 p.
2. Introduction to algorithms / Thomas H. Cormen. 3rd ed. – The MIT Press Cambridge, Massachusetts London, England, 2019. – 1313 p.

Extra

3. Skiena, Steven S. The Algorithm design manual 3rd ed. – Springer, 2020. – 793 s.
4. Kurt Mehlhorn, Peter Sanders Algorithms and Data Structures The Basic Toolbox. – Springer, 2018. – 295 s.
5. Allen B. Downey Think Data Structures: Algorithms and Information Retrieval in Java 1st Edition. – Springer, 2018. – 158 s.

Information resources.

8. Site of personal educational systems SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS discipline "Algorithm development and analysis" <https://pns.hneu.edu.ua/course/view.php?id=8597>