МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№02071211

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

ОСНОВИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

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

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№02071211

FUNDAMENTALS OF MATH MODELING
working program of the educational discipline

Field of knowledge	**12 "INFORMATION TECHNOLOGIES"**
Specialty	**125 "CYBER SECURITY"**
Educational level	**first (bachelor's)**
Educational program	**CYBER SECURITY**

Discipline status	mandatory
Teaching language	English

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

Olha STARKOVA

Kharkiv
2022

APPROVED
at the meeting of the department of *cyber security and information technologies*
Protocol № 1, August 27, 2022

Developer:
Olena Shapovalova, Ph.D., Assoc. Department of CAT

Renewal and Re-Approval Letter
work program of the academic discipline

Educational year	Date meeting department - developer of RPND	Number protocol	Signature manager department

Abstract of the academic discipline

The task of the educational discipline "Fundamentals of math modeling" is the formation of skills and competencies in the field of development and application of models for researching the level of cyber security of information systems. Teaching the discipline involves familiarizing students with the basic concepts of mathematical modeling and the formalized recording of security policy rules, acquiring the skills to compile and analyze mathematical models on the basis of statistical data processing, mastering the use of classic models: statistical, regression, optimization, discretionary, mandated and role-based access, etc.

The educational discipline "Fundamentals of math modeling" is an important component of the cycle of computer disciplines for the training of bachelors in the specialty "Cybersecurity".

The subject of the discipline is mathematical models of cyber security as well as modern methods of their developments and analysis, in particular, regression and correlation analysis of data, access control techniques.

The goal of the educational discipline "Fundamentals of math modeling" is to provide higher education students with theoretical knowledge of the Fundamentals of math modeling of objects from the point of view of their cyber security, students' assimilation of the main approaches and principles of creating models and the acquisition of skills in their application to analyze the level of cyber security of information systems; acquiring skills in using methods of formulating and solving modeling problems and analyzing their complexity; understanding of the essence of mathematical support of information systems; creating and implementation of mathematical models of information processing processes, their optimization and determination of areas for improvement.

The results of studying the discipline are systematic knowledge and practical skills in the field of development and application of mathematical models for processing statistical data, evaluating the quality of obtained models and solving problems of cyber security.

Characteristics of the academic discipline

Course	**3**
Semester	**1**
ECTS credits number	**4**
Final control form	**credit**

Structural and logical scheme of study of the academic discipline:

Prerequisites	Post-requisites
Higher mathematics	Foundations cryptographic protection
Methods and means computer informative technologies	Foundations technical protection information
Technologies processing information	Software informative security

Competencies and learning outcomes by 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. 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. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, 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 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 information and/or cyber security policy.	LO 9 – to implement processes, based on national and international standards, of detection, identification, analysis and response to information and/or cyber security incidents ;
CS 7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, 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 information and/or cyber security policy.	LO 12 – develop threat and offender models;
CG 5. Ability to search, process and analyze information. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. 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.	LO 13 – analyze projects of information and telecommunication systems based on standardized technologies and data transfer protocols

CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the 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 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 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 functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 14 – solve the task of protecting programs and information processed in information and telecommunication systems by software and hardware and evaluate the effectiveness of the quality of the decisions made
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 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 15 – use modern software and hardware of information and communication technologies
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 regulatory, 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 information and/or cyber security policy.	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 objective areas and understanding 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 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 functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 17 – to ensure the 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 information resources with a display of relationships and information flows, processes for internal and remote components;
KZ 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 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 18 – use software and hardware complexes for the protection of information resources
KZ 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.	LO 20 – to ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems

CS 10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.	
CG 5. Ability to search, process and analyze information. 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 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 28 – to analyze and evaluate the effectiveness and level of security of resources of various classes in information and information-telecommunication (automated) systems during testing in accordance with the established policy of information and/or cyber security systems based on access control models (mandatory, discretionary, role-based);
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 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 information and/or cyber security policy.	LO 29 – to evaluate the possibility of realization of potential threats of information processed in information and telecommunication systems and the effectiveness of the use of complexes of protection means in the conditions of realization of threats of various classes;
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 information and/or cyber security policy.	LO 30 – carry out an assessment of the possibility of unauthorized access to elements of information and telecommunication systems;
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 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. 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.	LO 33 – to solve the tasks of ensuring the continuity of business processes of the organization based on the theory of risks;

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 information and/or cyber security policy.	
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 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 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 information and/or cyber security policy.	LO 34 – participate in the development and implementation of information security and/or cyber security strategy in accordance with the goals and objectives of the organization;
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. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, 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 information and/or cyber security policy.	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 and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security ;
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	LO 42 – to implement the processes of detection, identification, analysis and response to information

purpose of implementing the established information and/or cyber security policy. 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 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 information and/or cyber security policy.	and/or cyber security incidents ;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. 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 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 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 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 information and/or cyber security policy.	LO 43 – apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents;
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 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 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	LO 44 – to solve the problems of ensuring the continuity of the organization's business processes on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards;

information resources in accordance with the established information and/or cyber security policy.	
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 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 information and/or cyber security policy.	LO 45 – apply early classes of information security and/or cyber security policies based on risk-oriented control of access to information assets;
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 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 information and/or cyber security policy.	LO 46 – to analyze and minimize the risks of information processing in information and telecommunication systems;
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 10. Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity.	LO 47 – to solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information
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 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment.	LO 50 – to ensure) the functioning of software and software-hardware intrusion detection complexes of various levels and classes (statistical, signature, statistical-signature)

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	
CG 1. Ability to apply knowledge in practical situations. CG 4. The ability to identify, pose and solve problems in a professional direction. 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 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 information and/or cyber security policy.	LO 53 – to solve the problems of software code analysis for the presence of possible threats.

Curriculum

Content module 1. Theoretical foundations of mathematical modeling

Topic 1. Introduction. Concept of mathematical modeling. Field of application, terminology. Types of models, classification, modeling stages.

Topic 2. Basic concepts of mathematical modeling, statistical data processing. Detection of correlation.

Topic 3. Regression models. The method of least squares. Linear paired regression model. Checking it for adequacy

Topic 4. Identification of mathematical model parameters. Multifactor model. Checking it for adequacy

Topic 5. Conditions for the correctness of building models. Special cases: multicollinearity, heteroscedasticity, autoregression.

Content module 2. Security models of computer systems

Topic 6. Data testing to detect heteroskedasticity.

Topic 7. Optimization models

Topic 8. Security policies. Types of models

Topic 9. Models of computer systems with discretionary access control

Topic 10. Models of computer systems with mandated access control

Topic 11. Models of computer systems with role-based access control.

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

Teaching the discipline involves the involvement of explanatory and illustrative (Topic 1, 2, 3, 6, 7), reproductive(Topic 4,5,6) , research (Topic 5, 6, 7) methods, as well as methods of problem-based learning (Topic 8-10) . Thus, during lectures, the teacher provides applicants with a significant amount of theoretical material with explanations involving graphic presentation (schemes, tables, presentations), proofs of mathematical hypotheses and formulas, examples of problem solving (Topic 2,3,4,5,6). During the laboratory classes, applicants have the opportunity to acquire practical problem-solving skills based on the problem formulated according to the subject of the class.

The given teaching methods are aimed at forming the ability of students to solve complex problems in the field of mathematical modeling.

The procedure for evaluating learning outcomes

The program of the academic discipline provides for lecture, laboratory and independent types of work. The knowledge and competences acquired by students during lecture classes are evaluated for writing control papers and taking tests, skills acquired during laboratory classes are evaluated for solving problems provided by the subject of the classes. Independent work is not evaluated separately, since it consists in preparation for other types of classes and is an integral component of obtaining an education. The evaluation of the developed competences of the applicants is carried out according to the accumulative 100-point rating system. Control measures include:

- current control, which is carried out during the semester during lectures and laboratory classes and is evaluated by the sum of points scored (the maximum sum is 100 points; the minimum sum that gives the student the opportunity to take a credit is 60 points);

- module control involves the completion of final control tasks, which may include a creative research component and require knowledge and skills acquired during the study of the set of material on the subject of the module.

Under the current control, the knowledge of the acquirers is evaluated according to the following criteria:

– fluent command of the educational material in its entirety, with an understanding of examples and the possibility of giving one's own examples to explain the essence of the material;

– demonstration of skills in applying methods of building mathematical models for solving applied problems;

– demonstration of skills in applying innovative work methods during problem solving;

– demonstration of the skills of searching and analyzing sources of information, substantiating the obtained results and forming conclusions at work;

– demonstration of teamwork skills when solving complex tasks on the development and analysis of mathematical models.

The formation of tasks and the control of their execution are aimed at helping students acquire the skills of active creative thinking, inculcating cognitive skills and norms of virtuous cooperation. The main requirement for the performance of tasks is the independence of their performance or determination of the percentage of contribution under the conditions of teamwork.

The distribution of current assessment points by types of work is as follows.

Lecture classes: the level of mastery of theoretical knowledge is determined during the defense of laboratory work, for writing test papers (the maximum number of points is 20).

Laboratory classes: the level of acquired skills in the application of knowledge to solve problems is determined by the correct performance of laboratory work tasks (the maximum number of points is 80).

Independent work: the level of mastery of the skills of using the latest knowledge, methodology and methods of conducting scientific research is determined by the degree of preparation of the applicant for the performance of laboratory and writing control papers (in the Rating Plan of the academic discipline, additional points for this type of work are not provided).

The applicant should be considered certified if the sum of points obtained as a result of the final/semester performance check is equal to or exceeds 60. The minimum possible number of points for current and modular control during the semester is 60 points. The total result in points for the semester is: "60 and more points - counted", "59 and less points - not counted" and entered in the "Performance record" of the educational discipline.

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

Rating-plan of the educational discipline

Topic	**Forms and species teaching**		**Forms assessment**	**Max score**
Topic 1	*Auditorium work*			
	Lecture	Lecture 1 ″ Introduction. Concept mathematical modeling. Branch application, terminology. Types models, classification, stages modeling. ″		
	Laboratory occupation	Laboratory work 1. Processing statistical data.		
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to performance of laboratory work. Implementation laboratory tasks		
Topic 2	*Auditorium work*			
	Lecture	Lecture 2 ″ Basic concepts mathematical modeling, processing statistical data. Detection correlations ″		

	Laboratory occupation	Laboratory work 1. Processing statistical data and detection correlations.	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 3	*Auditorium work*			
	Lecture	Lecture 3 " Regression models. Method the smallest squares. Linear even regressive model. Multifactorial model. Rating quality modeling »		
	Laboratory occupation	Laboratory work 2. Linear even regressive model.	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 4	***Auditorium work***			
	Lecture	Lecture 4 " Conditions correctness buildings models. special cases : multicollinearity, heteroskedasticity, autoregression. "	Control work 1	5
	Laboratory occupation	Laboratory work 3. Regressive models. Calculation parameters steam room regression, verification quality models.	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 5	***Auditorium work***			
	Lecture	Lecture 5 " Testing data with a purpose detection multicollinearity		

		and her elimination »		
	Laboratory occupation	Laboratory work 4. Regressive models. Calculation parameters multifactorial regression, verification quality models.	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 6	***Auditorium work***			
	Lecture	Lecture 6 ″ Testing data with a purpose detection heteroscedasticity ″		
	Laboratory occupation	Laboratory work 5. Detection multicollinearity in the data and her elimination	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 7	***Auditorium work***			
	Lecture	Lecture 7 ″ Optimization models ″	Control work 1	5
	Laboratory occupation	Laboratory work 6. Testing data with a purpose detection heteroscedasticity	Protection laboratory work	8
	Independent work			

	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 8	***Auditorium work***			
	Lecture	Lecture 8 ″ Politicians security. Types models ″		
	Laboratory occupation	Laboratory work 7. Optimization models. Optimization planning production	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 9	***Auditorium work***			
	Lecture	Lecture 9 ″ Models computer systems with discretionary management access _ Model of Khru ″		
		Lecture 10 ″ Models computer systems with discretionary management access _ Take-Grand Model ″		
	Laboratory occupation	Laboratory work 8. Optimization models. Transport problem	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic	***Auditorium***			

10	***work***			
	Lecture	Lecture 11 ″ Models computer systems with a mandate management access _ Model Bella LaPadula ″		
	Laboratory occupation	Laboratory work 9. Models computer systems with discretionary management access _ Model of Khru. Take-Grand model	Protection laboratory work	8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to implementation laboratory works _ Implementation laboratory tasks		
Topic 11	***Auditorium work***			
	Lecture	Lecture 12 ″ Model role-playing access ″	Control work 3	10
	Laboratory occupation	Laboratory work 10. Model mandated access _ Model Bella LaPadula		8
	Independent work			
	Question and task to independent processing	Search, selection and review literary sources by given subject matter. Preparation to		

References

Basic

1 Brooks C. J., Grow, C., Craig, P., & Short, D. Cybersecurity essentials. – John Wiley & Sons, 2018. – 767 p.

2 Johnson T. A. (ed.). Cybersecurity: Protecting critical infrastructures from cyberattack and cyber warfare. – CRC Press, 2019. – 346p.

3 The C Programming Language The Ultimate Beginner’s Guide. EasyProgramming Publisher, 2020. – 151p.

4 Aumasson J.-P. Serious Cryptography. A Practical Introduction to Modern Encryption. No Starch Press. 2018. – 434p.

5 Seacord R.C. Effective C. An introduction to Professional C Programming. – No Starch Press, 2020. – 305p.

Optional

6 Lehto M., Neittaanmäki P. (ed.). Cyber security: Analytics, technology and automation. – Springer, 2019. – Т. 78. – 258 p.

7 Hall G., Watson E. Computer Hacking, Security Testing, Penetration Testing and Basic Security. –

8 Chio C., Freeman D. Machine learning and security: Protecting systems with data and algorithms. – " O'Reilly Media, Inc.", 2018. – 385p.

9 Bowne S. Hands-On Cryptography with Python. – Packt. 2018. – 124 p.

10 Nikolayeva O.G., Shapovalova O.O. Laboratory workshop on the disciplines "Simulation modeling" and "System analysis": Educational and methodological manual. - Kharkiv: KhNUBA, 2020 – 110 p.

Information resources on the Internet

11 Site of personal educational systems of Khnei National University named after S. Kuznets in the discipline "Fundamentals of math modeling" https://pns.hneu.edu.ua/course/view.php?id=8584

12 https://www.voxco.com/survey-feature/correlation-analysis/

13 https://www.google.com/search?q=correlation+analysis&clien