МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна ПЕМАШКАЛО

ТЕХНОЛОГІЇ УПРАВЛІННЯ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ

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

BUSINESS PROCESS SECURITY MANAGEMENT TECHNOLOGIES

work program of the educational discipline

Field of expertise	**12 "Information technology"**
Specialty.	**125 "Cybersecurity"**
Educational level	**first (bachelor's)**
Educational program	**"Cybersecurity"**

Status of the discipline	**mandatory**
The language of teaching, learning and assessment	**English**

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

Kharkiv

2022

APPROVED
at a meeting of the Department of *Cybersecurity and Information Technology*
Minutes No. 1 dated 08/27/2022.

Developer:
Dolgova N.G., PhD, Associate Professor of KIT,

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

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

Summary of the subject

The tools for presenting existing and constantly updated knowledge are widely used in the modern IT tools market, as they provide a more visual and convincing reflection of the processes of our time, help to expand the audience of those interested and identify specific requirements for the material presented.

The subject of the discipline is the basic definitions and concepts of knowledge engineering and neuroinformatics, the main tasks and methods of knowledge engineering and methods of representation and processing of knowledge. The objects of study are knowledge as a subjective category, the relationship with the concepts of data and information, methods of formalizing knowledge, including fuzzy knowledge, methods of solving problems in knowledge-based systems, methods of knowledge acquisition, architecture of expert systems as one of the types of intelligent information systems and tools for developing knowledge bases.

The purpose of the discipline "Business Process Security Management Technologies" is to form a systematic basic understanding, primary knowledge, skills and abilities of students on the basics of business process security management technologies as one of the areas of building security systems, to give an idea of business process models and modeling methods based on the process approach.

The results of studying the discipline are the acquisition of skills and abilities to navigate different methods of knowledge representation, transitions from one method to another, formalization of expert knowledge using different methods of knowledge representation, development of a product knowledge base for solving problems of choosing options in a poorly formalized subject area and programming in the Prolog language.

Characteristics of the discipline

Course.	**3**
Semester	**5**
Number of ESTS credits	**5**
Form of final control	**examination**

Structural and logical scheme of studying the discipline

Prerequisites	Post requisites
Information security management	Organizational support of information security

Competencies and learning outcomes in the discipline

Competencies	Learning outcomes
CG 1. Ability to apply knowledge in practical situations. LO 2. Knowledge and understanding of the subject area and understanding of the profession. CG 3. Ability to communicate professionally in the state and foreign languages both orally and in writing.	LO 1 - apply knowledge of state and foreign languages to ensure the effectiveness of professional communication;
CG 1. Ability to apply knowledge in practical situations. LO 2. Knowledge and understanding of the subject area and understanding of the profession. CG 4. Ability to identify, formulate and solve problems in the professional field.	LO 2 - organize own professional activity, choose the best methods and ways to solve complex specialized tasks and practical problems in professional activity, evaluate their effectiveness;

CG 5. Ability to search, process and analyze information	LO 3 - use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity; LO 4 - analyze, argue, make decisions in solving complex specialized tasks and practical problems in professional activities characterized by complexity and incomplete certainty of conditions, and be responsible for the decisions made;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CG 4. Ability to identify, formulate and solve problems in the professional field. CG 5. Ability to search, process and analyze information	LO 5 - to adapt to the conditions of frequent changes in the technologies of professional activity, to predict the final result;
CG 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 6 - critically comprehend the basic theories, principles, methods and concepts in learning and professional activities;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CG 4. Ability to identify, formulate and solve problems in the professional field. CS 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity.	LO 7 - act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cybersecurity;
CG 5. Ability to search, process and analyze information. PC 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems.	LO 9 - implement processes based on national and international standards for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents;

CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practices, etc.) CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them.	LO 14 - to solve the problem of protecting programs and information processed in information and telecommunication systems by software and hardware and to assess the effectiveness of the quality of decisions made;

CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools 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 information and/or cybersecurity policy.	LO 15 - use modern software and hardware of information and communication technologies;
CG 2. Knowledge and understanding of the subject area and understanding of the profession. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at the objects of information activity.	LO 17 - to ensure the processes of protection and operation of information and telecommunication (automated) systems based on practices, skills and knowledge of structural (structural and logical) schemes, network topology, modern architectures and models of protection of electronic information resources with the reflection of interconnections and information flows, processes for internal and remote components;

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	
CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 18 - use software and hardware and software systems to protect information resources;
CG 1. Ability to apply knowledge in practical situations. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities.	LO 20 - to ensure the functioning of special software to protect information from destructive software influences, destructive codes in information and telecommunication systems;

CG 1. Ability to apply knowledge in practical situations. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 21 - to solve the tasks of providing and maintaining (including: review, testing, accountability) the access control system in accordance with the established security policy in information and information and telecommunication (automated) systems;
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 24 - to solve problems of access control to information resources and processes in information and information and telecommunication (automated) systems based on access control models (mandatory, discretionary, role-based);
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin.	LO 25 - to analyze and evaluate the effectiveness and level of security of resources of different classes in information and information and telecommunication (automated) systems during tests in accordance with the established information and/or cybersecurity policy;

CG 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 33 - to solve the problems of ensuring the continuity of the organization's business processes based on risk theory;
CG 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 34 - To participate in the development and implementation of the information security and/or cybersecurity strategy in accordance with the goals and objectives of the organization;
CG 1. Ability to apply knowledge in practical situations. PC 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in	LO 35 - to solve the problems of providing and maintaining integrated information security systems, as well as counteracting unauthorized access to information resources and processes in information and information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy;

information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 7. Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organizational and technical means and methods, procedures, practices, etc.) CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	

CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	LO 42 - implement processes for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents;
CG 2. Knowledge and understanding of the subject area and understanding of the profession.	LO 43 - apply national and international regulations in the field of information

CS 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	security and/orcybersecurity to investigate incidents;

CG 1. Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cybersecurity. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 44 - to solve the problems of ensuring the continuity of the organization's business processes based on the risk theory and the established information security management system, in accordance with national and international requirements and standards;

CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 45 - apply different classes of information security and/or cybersecurity policies based on risk-based access control to information assets;
CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 9. Ability to carry out professional activities on the basis of the implemented information and/or cybersecurity management system. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 46 - to analyze and minimize 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 cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy.	LO 47 - to solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic information protection;

CS 10. Ability to apply methods and means of cryptographic and technical protection of information at information activities.	

CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them. CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy.	LO 50 - to ensure) the functioning of software and hardware intrusion detection systems of various levels and classes (statistical, signature, statistical-signature)

CG 1. Ability to apply knowledge in practical situations. CG 4. Ability to identify, formulate and solve problems in the professional field. 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 cybersecurity. CS 3. Ability to use software and hardware complexes of information security tools in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy. CS 5. Ability to ensure the protection of information processed in information and telecommunication (automated) systems in order to implement the established information and/or cybersecurity policy. CS 6. Ability to restore normal functioning of information, information and telecommunication (automated) systems after threats, cyber attacks, failures and failures of various classes and origin. CS 8. Ability to implement incident management procedures, conduct investigations, and evaluate them.	LO 53 - to solve problems of analyzing program code for possible threats;

CS 11. Ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established information and/or cybersecurity policy. CS 12. Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy	

CG 1. Ability to apply knowledge in practical situations. LO 2. Knowledge and understanding of the subject area and understanding of the profession. CG 6. The ability to exercise their rights and responsibilities as a member of society, to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine. CG 7. Ability to preserve and increase moral, cultural, scientific values and achievements of society based on an understanding of the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, technology and technology, to use various types and forms of physical activity for active recreation and healthy lifestyle	LO 54 - to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine

Program of the discipline

Content module 1: Introduction to business process security management

Topic 1: Functional and process approaches to business process security management
Topic 2. Theoretical foundations of business process management
Topic 3. Business process and its components
Topic 4. Reference and benchmark models
Topic 5. Methodologies for describing activities

Content module 2: Business process security management tools

Topic 6: Tool systems for business modeling
Topic 7. Methods of describing different subject areas
Topic 8: Methods of process analysis
Topic 9: Process control and monitoring
Topic 10. Process transformation and process organization

The list of laboratory classes, as well as questions and assignments 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 and illustrative (information and receptive) and reproductive teaching methods. As teaching methods aimed at

activating and stimulating the educational and cognitive activities of students, problematic lectures (topics 1-10), presentations (topics 1-10), laboratory work (topics 1, 3, 5, 7, 9) are used.

The procedure for assessing learning outcomes

The program of the discipline includes lectures, laboratory and independent work. The knowledge and competencies acquired by students during lectures are assessed by writing quizzes and taking tests, and the skills acquired during laboratory classes are assessed by solving problems related to the subject matter of the classes. Independent work is not assessed separately, as it is a preparation for other types of classes and is an integral part of education. The assessment of the formed competencies of applicants is carried out according to a cumulative 100-point rating system. Control measures include

- current control, which is carried out during the semester during lectures and laboratory classes and is assessed by the amount of points scored (maximum amount - 60 points; minimum amount of admission to the exam - 35 points)

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

During the current control, students' knowledge is assessed according to the following criteria

- fluency in the full scope of the training material, with an understanding of the examples and the ability to provide their own examples to explain the essence of the material;

- demonstration of skills in applying methods of building mathematical models to solve applied problems;

- demonstration of skills in applying innovative methods of work in solving problems;

- Demonstration of skills in searching and analyzing information sources, justifying the results obtained, and drawing conclusions in the work;

- demonstration of teamwork skills in solving complex problems in the development and analysis of mathematical models.

The formation of tasks and control over their implementation are aimed at helping students acquire active creative thinking skills, instilling cognitive skills and norms of fair cooperation. The main requirement for completing assignments is to complete them independently or to determine the percentage of contribution in teamwork.

The distribution of points in the current assessment by type of work is as follows.

Laboratory classes: the level of mastery of theoretical knowledge is determined during lectures, writing quizzes (maximum number of points is 10) and express questioning (maximum number of points is 10). The level of acquired skills in applying knowledge to solve problems is determined by the correctness of the tasks of laboratory work (the maximum number of points is 40).

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 graduate student for laboratory work and writing tests (the technological map does not provide additional points for this type of work).

Final control: is carried out taking into account the exam.

The exam paper covers the program of the discipline and provides for determining the level of knowledge and the degree of competence of students. Each examination paper consists of 2 theoretical questions and 1 practical task, which involve solving typical professional tasks of a specialist in the workplace and allow to diagnose the level of theoretical training of the student and the level of his/her competence in the discipline. The assessment of each task of the examination paper is as follows: the first theoretical question is worth 10 points; the second question is worth 10 points; the third practical task is a calculation task, its completion is worth 20 points.

The result of the semester examination is evaluated in points (maximum number of points - 40 points, minimum number of points - 25 points) and is put in the appropriate column of the examination "Record of academic performance". An applicant should be considered certified if the sum of points obtained as a result of the final/semester academic performance test is equal to or

exceeds 60. The minimum possible number of points for the current and module 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 exam and the points obtained during the current control under the cumulative system. The total result in points for the semester is: "60 and more points - passed", "59 and less points - failed" and is entered into the academic record of the discipline.

The forms of evaluation and the distribution of points are shown in the table "Rating plan of the discipline".

Rating plan of the discipline

Topic.	Forms and types of training		Evaluation forms	Max score
Topic 1	***Audit work***			
	Problematic lecture	Problem lecture "Functional and process approaches to business process security management"		
	Laboratory lesson	*Laboratory work №1.* Description of the system built on the concept of "Process Improvement"	Performing laboratory work	
			Defense of laboratory work № 1	8
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 2	***Audit work***			
	Problematic lecture	Lecture "Theoretical foundations of business process management"		
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 3	***Audit work***			
	Problematic lecture	Lecture "Business process and its components"		
	Laboratory lesson	Laboratory work #2. Description of the system built on the concept of "Process formalization"	Performing laboratory work Defense of laboratory work № 3	8
	Independent work			

	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 4	***Audit work***			
	Problematic lecture	Lecture "Reference and reference models"		
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 5	***Audit work***			
	Problematic lecture	Lecture ″Methodologies for describing activities″	Express survey	5
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 6	***Audit work***			
	Problematic lecture	Lecture ″Instrumental systems for business modeling″		
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 7	***Audit work***			
	Problematic lecture	Lecture ″Methods of describing different subject areas″		
	Laboratory lesson	Laboratory work #3. Organization of management of end-to-end processes and groups of processes	Performing laboratory work	
			Defense of laboratory work № 3	8
			Control work 1	5
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		

Topic 8	***Audit work***			
	Problematic lecture	Lecture ″Methods of process analysis″		
	Laboratory lesson	Laboratory work №4 Building a system of organization processes based on value chain analysis	Performing laboratory work	
			Defense of laboratory work № 4	8
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 9	***Audit work***			
	Problematic lecture	Lecture ″Controlling and monitoring of processes″		
			Express survey	5
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
Topic 10	***Audit work***			
	Problematic lecture	Lecture ″Process transformation and process organization″		
	Laboratory lesson	Laboratory work №5 Analysis of the topology of the security management process		
			Defense of laboratory work № 5	8
			Control work 2	5
	Independent work			
	Questions and tasks for independent study	Search, selection, and review of literature on a given topic. Preparation for laboratory work. Performing laboratory tasks		
	Examination			40
	Total points			100

Recommended reading

Basic

1. Cybersecurity and information technology. - Kh.; DISA PLUS LLC, 2020. -380 c.
2. Information security and information technology. - Kh.; DISA PLUS LLC, 2019. - 322 c.

Additional

3. Kostina O. M. Diagnostics and management of business processes in the context of enterprise crisis management / Electronic scientific edition "Ekonomika i suspilstvo".2019. № 10 - C. 287-297.
4. Md Imtiaz Mostafiz, Murali Sambasivan, See Kwong Goh, (2019) "Impacts of dynamic managerial capability and international opportunity identification on firm performance", Multinational Business Review, 13. Prodius O.I., Naida E.D. Business process reingineering as a modern management concept // Electronic scientific edition "Ekonomika ta suspilstvo" 2019.

Information resources.

5. Website of personal learning systems of KhNUE named after S. Kuznets in the discipline "Technologies of business process security management" https://pns.hneu.edu.ua/course/view.php?id=8952