СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

NPJSC "Kazakh National Research Technical University named after K. Satpayev"
Institute of Cybernetics and Information Technology
Department of Cybersecurity, Information Processing and Storage

CURRICULUM PROGRAM

7M06104 - «COMPREHENSIVE INFORMATION SECURITY SUPPORT »

(Scientific and pedagogical direction, 2 years)

Master of Technical Sciences

2st edition
in accordance with the State Educational Standard of Higher Education 2018

Almaty 2020

The program was drawn up and signed by the parties:

About KazNRTU named after K.I. Satpayev:

Director of the Institute of Cybernetics and Information Technology	N.A. Seilova
Head of the Department of Cybersecurity, processing and storage of information "(CPaSI)	N.A. Seilova
Chairman of the UMG of the Department of CPaSI	E.Zh. Aytkhozhaevva

From employers:

Department Director of Kazteleport LLP S. Toleuliv

From partner university:
National Aviation University (NAU, Kiev, Ukraine)

Approved at a meeting of the Educational and Methodological Council of the Kazakh National Research Technical University named after K.I. Satpayev. Minutes No. 3 dated 15.12.2020

Qualification:
Level 7 of the National Qualifications Framework:

Professional competence: Comprehensive information security, Information security audit, Organization of information security systems.

1 Brief description of the program:

1 Purpose of the educational program: The purpose of the educational program is to train undergraduates in the scientific and pedagogical direction. The educational program includes basic and specialized disciplines with the achievement of relevant competencies, as well as the passage of various types of practices (research, experimental, pedagogical and internships).

The professional activity of the masters is aimed at the protection and security of information, namely, the integrated provision of information security and engineering and technical protection of information.

Training of masters of scientific and pedagogical direction in information security will be carried out according to the new educational program (EP) "Comprehensive information security". The programs of disciplines and modules of the educational program are interdisciplinary and multidisciplinary in nature, are developed taking into account the relevant educational programs of the world's leading universities and the international classifier of professional activities in the direction of information security.

The educational program "Comprehensive Information Security" is developed on the basis of the main regulatory documents:

- The Law of the Republic of Kazakhstan "On Education" dated July 27, 2007 No. 319-III with amendments and additions dated October 24, 2011 No. 487-VI ЗРК;
- Rules for organizing the educational process on credit technology of education, approved by the Order of the Minister of the Ministry of Education and Science of the Republic of Kazakhstan No. 152 dated April 20, 2011 (the last changes were introduced by the Order of the Minister of the Ministry of Education and Science of the Republic of Kazakhstan No. 90 dated January 28, 2016);
- State compulsory education standard for all levels of education, order No. 604 dated 31.10.2018 and No. 182 dated 05.05.2020.
- National qualifications framework. Approved by the protocol of March 16, 2016 by the Republican Tripartite Commission on Social Partnership and Regulation of Social and Labor Relations;
- Sectoral Qualifications Framework (SQF). Approved by the protocol of November 17, 2016 No. 12-03-333 of the Sectoral Commission on Social Partnership and Regulation of Social and Labor Relations in the Electric Power Industry;
- Typical curriculum 6M100200 - Information security systems, approved by the Order of the Minister of the Ministry of Education and Science of the Republic of Kazakhstan No. 425 dated 05.07.2016
- Recommendation of the International Association for Computing Machinery (ACM) Curriculum in Computer Science (CC2005 series).

The master of the educational program "Integrated information security" is focused on the independent determination of the goal of professional activity and the choice of adequate methods and means of achieving them, the implementation of scientific, innovative activities to obtain new knowledge. In addition, it is focused on the organization, design, development, management and audit of systems for the protection and security of information for applied purposes for all sectors of the economy, government organizations and other areas of activity.

The program is designed to implement the principles of the democratic nature of education management, to expand the boundaries of academic freedom and powers of educational institutions, which will ensure the training of qualified, highly motivated personnel for innovative and knowledge-intensive sectors of the economy.

The educational program provides an individual approach to students, the transformation of professional competencies from professional standards and qualifications standards into learning outcomes and ways to achieve them.

The educational program was developed on the basis of an analysis of the labor functions of an information security administrator, an information security auditor, an information security engineer, declared in professional standards.

Representatives of Kazakhstani companies and associations, specialists of departmental structures in the field of protection and security participated in the development of the educational program.

The objectives and content of the EP are given in section 9 "Description of disciplines".

The main criterion for the completion of training in Master's programs is the development of all types of educational and scientific activities of a master's student.

In case of successful completion of the full course, the master is awarded a master of technical sciences in the educational program "Integrated information security."

2 Types of work

- design and engineering;
- production and technological;
- experimental research;
- organizational and managerial;
- operational;
- scientific;
- research.

3 Objects of professional activity:

The objects of professional activity of the master are: audit and monitoring of information security; organization and technology of information protection; ensuring cryptographic protection of information; response to information security incidents; information security management systems; organizational support of information security audit; information security audit planning; support of information security systems during its operation.

2 PASSPORT OF THE EDUCATIONAL PROGRAM

1 Scope and content of the program

The term of study in the master's program is determined by the amount of acquired academic credits Upon mastering the established amount of academic credits and achieving the expected learning outcomes for obtaining a master's degree, the master's educational program is considered fully mastered. In the scientific and pedagogical magistracy, at least 120 academic credits must be mastered for the entire period of study, including all types of educational and scientific activities of the undergraduate.

The planning of the content of education, the way of organizing and conducting the educational process is carried out by the university independently on the basis of the credit technology of education.

The master's degree in scientific and pedagogical direction implements educational programs of postgraduate education for the preparation of scientific and scientific and pedagogical personnel for universities and scientific organizations with in-depth scientific, pedagogical and research training.

The content of the Master's degree program consists of:

1) theoretical training, including the study of cycles of basic and major disciplines;

2) practical training of undergraduates: various types of practices, scientific or professional internships;

3) research work, including the implementation of a master's thesis.

4) final certification.

Name: Comprehensive information security

The purpose of the educational program:

- Provide training for specialists in scientific activity and production in the field of information security, who are able to apply various technologies, knowledge, skills and competencies in the organization, management and design of information security systems.
- To prepare specialists in scientific, pedagogical activities and production for production activities related to the process of audit, monitoring, investigation of information security incidents, focused on the expected results.
- Prepare managers capable of organizational and managerial activities related to planning, development, operation and maintenance of information protection and security processes.
- Create conditions for continuous professional development, development of social and personal competencies, social mobility and competitiveness in the labor market.

Objectives of the educational program:

Training of highly qualified specialists who are able to solve the following tasks:

- planning of work on audit of information security;
- organizational support of information security audit;

-conducting an analysis of the compliance of design, operational and technical documentation on information security with the requirements in the field of ICT and IS provision of the IS audit object;

- analysis of the current state of security of the IS audit object;
- identification and elimination of vulnerabilities;
- monitoring and investigation of information security incidents;
- development of a model of threats to information security in enterprises;
- development of technical specifications for the creation of an information security system.

2 Requirements for applicants

The previous level of education of applicants is higher professional education (bachelor's degree). The applicant must have a diploma of the established sample and confirm the level of knowledge of the English language with a certificate or diplomas of the established sample.

The procedure for admitting citizens to the magistracy is established in accordance with the "Standard rules for admission to training in educational organizations that implement educational programs of postgraduate education."

The formation of a contingent of undergraduates is carried out by placing a state educational order for the training of scientific and pedagogical personnel, as well as paying for training at the expense of citizens' own funds and other sources. The state provides citizens of the Republic of Kazakhstan with the right to receive, on a competitive basis, in accordance with the state educational order, free postgraduate education, if they receive education of this level for the first time.

At the "entrance", a master's student must have all the prerequisites necessary for mastering the corresponding educational master's program. The list of required prerequisites is determined by the higher education institution independently.

In the absence of the necessary prerequisites, the master student is allowed to master them on a paid basis.

3 Requirements to complete the course and receive a diploma

Awarded degree / qualification: A graduate of this educational program is awarded a master's degree in technical sciences in the educational program "Integrated information security."

A graduate who has mastered master's programs must have the following general professional competencies:

- the ability to independently acquire, comprehend, structure and use new knowledge and skills in professional activities, develop their innovative abilities;
- the ability to independently formulate research goals, establish a sequence for solving professional problems;
- the ability to apply in practice the knowledge of fundamental and applied disciplines that determine the focus (profile) of the master's program;

- the ability to professionally choose and creatively use modern scientific and technical equipment for solving scientific and practical problems;

- the ability to critically analyze, represent, defend, discuss and disseminate the results of their professional activities;

- possession of the skills of drawing up and preparing scientific and technical documentation, scientific reports, reviews, reports and articles;

- willingness to lead a team in the field of their professional activities, tolerantly perceiving social, ethnic, confessional and cultural differences;

- readiness for communication in oral and written forms in a foreign language to solve problems of professional activity.

A graduate who has mastered the master's program must have professional competencies corresponding to the types of professional activities that the master's program is focused on:

research activities:

- the ability to form diagnostic solutions to professional problems by integrating the fundamental sections of science and specialized knowledge gained during the master's program;

- the ability to independently conduct scientific experiments and research in the professional field, generalize and analyze experimental information, draw conclusions, formulate conclusions and recommendations;

- the ability to create and research models of the studied objects based on the use of in-depth theoretical and practical knowledge in the field of information protection and security;

- research and production activities:

- the ability to independently carry out production and research and production, laboratory and interpretation work in solving practical problems;

- the ability to professionally operate modern laboratory equipment and instruments in the field of the mastered master's program;

- the ability to use modern methods of processing and interpreting complex information to solve production problems;

- project activities:

- the ability to independently compose and present projects of research and development work in the field of information security;

- readiness to design complex research and development work in solving professional problems;

- organizational and management activities:

- the willingness to use the practical skills of organizing and managing research and development work in solving professional problems;

- readiness for the practical use of regulatory documents in the planning and organization of scientific and industrial work in the field of information security;

- scientific and educational activities:

- the ability to conduct seminars, laboratory and practical classes;

- the ability to participate in the management of scientific and educational work of students in the field of information security.

4 Working curriculum of the educational program and modular educational program

4.1. Study period 2 years

Working curriculum of the educational program

Education program: 7M**06104 – «Comprehensive information security support»**

Duration of training: 2 years

Academic degree: Master of Technical Sciences

year of study	Code	Name of course	Component	Credits		lecture/ laboratory/ practice/ IWS	Prerequisites	Code	Name of course	Component	Credits		lecture/ laboratory/ practice/ IWS	Prerequisites
				ECTS	ME						ECTS	ME		
1	**1 semester**							**2 semester**						
	HUM 201	History and philosophy of science	BD IC	4	2	1/0/1/2		LNG202	Foreign language (professional)	BD IC	6	3	0/0/3/3	
	HUM 207	Higher school pedagogy	BD IC	4	2	1/0/1/2			Elective	PS CC	6	3		
		Elective	PS CC	6	3				Elective	PS CC	6	3		
		Elective	BD CC	6	3			HUM 204	Management psychology	BD IC	4	2	1/0/1/2	
	AAP 242	Master's student scientific research, including an internship and a master's thesis	MSSR	6					Elective	BD CC	6			
									Elective	BD CC	6			
								AAP244	Pedagogical practice	BD IC	6			
								AAP 242	Master's student scientific research, including an internship and a master's thesis	MSSR	6			
		In total		**26**					**In total**		**46**			
2	**3 semester**							**4 semester**						
	SEC 204	Information Security Audit	PS IC	6	3	2/1/0/3		AAP242	Master's student scientific research, including an internship and a master's thesis	MSSR	6			
		Elective	PS CC	5	3			AAP243	Research scientific training	PS	7			
		Elective	PS CC	5	3			ECA205	Registration and defense of the master's thesis (RaDMT)	FA	12			
		Elective	PS CC	5	3									

	AAP 242	Master's student scientific research, including an internship and a master's thesis	MSSR	6										
		In total		**30**					**In total**		**25**			
									In all		**125**			

ELECTIVE DISCIPLINE CATALOG
Educational program
Education program: 7M06104 – «Comprehensive information security support»

BD Choice component - 18 credits					
	Code	**Name of disciplines**	**Credits**	**Lec/lab/prac/IWS**	**Semester**
	SEC221	Means of security of network of operating systems	6	2/0/1/3	1
	CSE249	Model-Driven Software Engineering	6	2/0/1/3	
	SEC201	Algorithms of cryptographic protection of information	6	2/0/1/3	2
	SEC 238	Steganographic methods of information protection	6	1/1/1/3	
	SEC244	Security of Virtualization and Cloud Systems	6	2/1/0/3	2
	SEC 208	Technical protection of information	6	1/1/1/3	
		Total	**18**		
PS CC **Choice component - 42 credits**					
	SEC215	Organization of information security systems	6	1/1/1/3	1
	GEN200	Numerical Methods in Engineering	6	1/1/1/3	2
	SEC214	Organization of protection and safety of a database	6	2/0/1/3	2
	CSE746	Machine Learning & Deep Learning	6	2/0/1/3	3
	CSE720	Cybercrime and computer forensics	6	2/1/0/3	3
	SEC218	Programming of microcontrollers	6	2/1/0/3	3
	SEC245	Risk management in cyber security	6	2/0/1/3	3
	SEC206	Security of systems of electronic business	6	2/1/0/3	3
	SEC246	Big Data and Data Analysis	6	2/1/0/3	3
		Total	**36**		

MODULAR CURRICULUM

Education program: 7M**06104 – «Comprehensive information security support»**

Form of study: daytime
Duration of training: 2 years
Academic degree: Master of Technical Sciences

The cycle	code	Name of disciplines	Semester	Acad. credits	lec.	lab.	prac	IWS	Type of contro	Chair
Profile training module										
Basic disciplines (BD) (40 credits)										
University component (18 credits)										
BD	HUM201	History and philosophy of science	1	4	1	0	1	2	Exam	SD
BD	HUM207	Higher school pedagogy	1	4	1	0	1	2	Exam	SD
BD	LNG202	Foreign language (professional)	2	6	0	0	3	3	Exam	EL
BD	HUM204	Management psychology	2	4	1	0	1	2	Exam	SECPM
Practice-oriented module										
	AAP244	Pedagogical practice	2	4	0	0	2	2	Report	
Choice component (18 credits)										
Module for network security and cloud technologies and cryptographic protection of information										
BD	SEC221	Means of security of network of operating systems	1	6	2	0	1	3	Exam	CIPaS
BD	SEC249	Model-Driven Software Engineering	1	6	2	0	1	3	Exam	CIPaS
BD	SEC201	Algorithms of cryptographic protection of information	2	6	2	0	1	3	Exam	CIPaS
BD	SEC 238	Steganographic methods of information protection	2	6	1	1	1	3	Exam	CIPaS
BD	SEC244	Security of Virtualization and Cloud Systems	2	6	2	1	0	3	Exam	CIPaS
BD	SEC 208	Technical protection of information	2	6	1	1	1	3	Exam	CIPaS
Major disciplines (MD) (49 credits)										
University component (6 credits)										
Module of scientific research, organization of information security system and ensuring information security										
MD	SEC204	Information Security Audit	3	6	2	1	0	3	Exam	CIPaS
Choice component (CC) (36 credits)										
MD	SEC215	Organization of information security systems	1	6	1	1	1	3	Exam	CIPaS
MD	GEN200	Numerical Methods in Engineering	2	6	1	1	1	3	Exam	AMaEG
MD	SEC214	Organization of protection and safety of a database	2	6	2	0	1	3	Exam	CIPaS
MD	CSE746	Machine Learning & Deep Learning	3	6	2	0	1	3	Exam	SE
MD	CSE720	Cybercrime and computer forensics	3	6	2	1	0	3	Exam	CIPaS
MD	SEC218	Programming of microcontrollers	3	6	2	1	0	3	Exam	CIPaS
MD	SEC245	Risk management in cyber security	3	6	2	0	1	3	Exam	CIPaS
MD	SEC206	Security of systems of electronic business	3	6	2	1	0	3	Exam	CIPaS

MD	SEC246	Big Data and Data Analysis	3	6	2	1	0	3	Exam	CIPaS
Practice-oriented module										
MD	AAP236	Research practice	4	7					Report	
Research Module (24 credits)										
MSSR	AAP242	Master's student scientific research	1	6					Report	
MSSR	AAP242	Master's student scientific research	2	6					Report	
MSSR	AAP242	Master's student scientific research	3	6					Report	
MSSR	AAP242	Master's student scientific research	4	6					Report	
Module of final attestation (12 credits)										
FA	ECA205	Registration and defense of the master's thesis	4	12					Defense of dissertation	
			Total	**125**						

5 Descriptors of the level and amount of knowledge, abilities, skills and competencies

The requirements for the level of preparation of a master's student are determined on the basis of the Dublin descriptors of the second level of higher education (master's) and reflect the acquired competencies, expressed in the achieved learning outcomes.

Learning outcomes are formulated both at the level of the entire educational program of the master's program, and at the level of individual modules or academic discipline.

Descriptors reflect learning outcomes that characterize the student's abilities:

1) demonstrate developing knowledge and understanding in the studied field of information technology and information security;

2) apply at a professional level their knowledge, understanding and ability to solve problems in a new environment, in a broader interdisciplinary context;

3) collect and interpret information to form judgments, taking into account social, ethical and scientific considerations;

4) clearly and unambiguously communicate information, ideas, conclusions, problems and solutions, both to specialists and non-specialists;

5) learning skills necessary for independent continuation of further education in the studied field of information technology and information security.

6 Competences to complete the training

6.1 Requirements for the key competencies of graduates of the scientific and pedagogical magistracy must:

1) have an idea:

- about the role of science and education in public life;
- about current trends in the development of scientific knowledge;
- on topical methodological and philosophical problems of natural (social, humanitarian, economic) sciences;
- about the professional competence of a higher school teacher;
- about the contradictions and socio-economic consequences of globalization processes;
- about professional competence in the field of information protection and security;
- about the technology of virtualization of resources and platforms;
- on the intellectualization of information security means;
- about database protection technologies;
- about algorithms for cryptographic information protection;
- about big data analysis.

2) know:

- methodology of scientific knowledge;
- principles and structure of the organization of scientific activity;
- the psychology of students' cognitive activity in the learning process;
- psychological methods and means of increasing the efficiency and quality of education;
- algorithms for cryptographic information protection;

- IS standards and IT security assessment criteria;
- technologies for virtualization of resources and platforms and virtualization systems from leading manufacturers;
- threats and risks of virtualization systems, principles of building hypervisors and their vulnerabilities;
- organization of IP networks, structure of IP packets and IP protocols;
- internal organization of OS information carriers;
- methods and means of storing key information and encryption;
- types and principles of authentication;
- requirements for firewalls and intrusion detection systems;
- database protection technologies and methods for designing secure databases;
- organization of the database protection and safety system;
- methods and tools for active audit;
- engineering and technical protection of information.

3) be able to:

- use the knowledge gained for the original development and application of ideas in the context of scientific research;
- critically analyze existing concepts, theories and approaches to the analysis of processes and phenomena;
- to integrate the knowledge gained in different disciplines to solve research problems in new unfamiliar conditions;
- by integrating knowledge, make judgments and make decisions based on incomplete or limited information;
- to apply the knowledge of pedagogy and psychology of higher education in their teaching activities;
- apply interactive teaching methods;
- to carry out information-analytical and information-bibliographic work with the involvement of modern information technologies;
- think creatively and be creative in solving new problems and situations;
- be fluent in a foreign language at a professional level, allowing for research and teaching of special disciplines in universities;
- to summarize the results of research and analytical work in the form of a dissertation, scientific article, report, analytical note, etc .;
- apply algorithms for cryptographic information protection;
- apply IS standards and conduct an IT security assessment;
- use virtualization systems from leading manufacturers;
- identify threats and risks of virtualization systems;
- apply methods and means of storing key information and encryption;
- work with firewalls and intrusion detection systems;
- apply database protection technologies and secure database design methods;
- to organize a system of protection and safety of the database;
- apply methods and tools of active audit;
- apply big data analysis tools.

4) have skills:

- research activities, solving standard scientific problems;
- implementation of educational and pedagogical activities on credit technology of education;
- methods of teaching professional disciplines;
- the use of modern information technologies in the educational process;
- professional communication and intercultural communication;
- oratory, correct and logical design of your thoughts in oral and written form;
- organization and protection of database security;
- conducting an information security audit;
- application of algorithms for cryptographic information protection;
- identifying threats and counteracting them;
- work with Big Data;
- expanding and deepening the knowledge necessary for daily professional activities and continuing education in doctoral studies.

5) be competent:

- in the field of research methodology;
- in the field of scientific and scientific-pedagogical activities in higher educational institutions;
- in matters of modern educational technologies;
- in the implementation of scientific projects and research in the professional field;
- in the organization of information security systems;
- in conducting information security audit;
- in ensuring the information security of the organization;
- in ways to ensure constant updating of knowledge, expanding professional skills and abilities.

B – Basic knowledge, abilities and skills

B1- To be able to assess the security of network operating systems and study the principles and methods of developing software for information systems.

B2 – Know modern and promising directions for the development of cryptographic protection of information and apply it in practice.

B3 - Know the technologies of virtualization of resources and platform, be able to use virtualization systems from leading manufacturers and be competent in engineering and technical information security.

P – Professional competence:

P1 – Know the issues of organizing information security systems and be able to carry out work on integrated information security in practice.

P2 – Ability to solve applied problems using numerical methods in engineering

P3– Be able to organize a database protection and security system and apply database protection technologies.

P4 – Be competent in machine learning and deep learning models

P5- be competent in cybercrime and computer forensics, be able to identify threats and carry out work to prevent intrusions.

P6 - Be able to plan, design, program and debug programs in universal languages.

P7 - Know information security standards and IT security assessment criteria, be able to apply active audit methods and tools.

P8 – Be competent in questions about existing types of security threats in e-business. Ability to provide information security of automated banking systems.

O - Human, social and ethical competences

O1- Ability to work in a team, have organizational skills, set priorities, quickly learn new knowledge and skills, apply them in practice.

O2 - Be focused on achieving results, to effectively plan and organize their own development.

O3 - Ability to use English fluently as a means of business communication, a source of new knowledge in the field of information security.

C - Special and managerial competencies:

C1 - Independent management and control of the processes of labor and educational activities within the framework of the strategy, policy and goals of the organization, critical discussion of the problem, reasoning of conclusions and competent operation of information.

C2 - Independent management and control of the processes of labor and educational activities within the framework of the strategy, policy and goals of the organization, critical discussion of the problem, reasoning of conclusions and competent operation of information; the ability to motivate to solve certain tasks, the ability to be responsible for the result of work at the level of a division or enterprise.

C3 - The ability to demonstrate a set of skills in managing the work process, the ability to choose methods, techniques and evaluation criteria for obtaining results, distribute and delegate authority, form teams, and make decisions during the production process.

6.2 Requirements for the research work of a master student in a scientific and pedagogical magistracy:

1) corresponds to the profile of the master's educational program, according to which the master's thesis is carried out and defended;

2) is relevant and contains scientific novelty and practical significance;

3) is based on modern theoretical, methodological and technological achievements of science and practice;

4) is carried out using modern scientific research methods;

5) contains research (methodological, practical) sections on the main protected provisions;

6) is based on advanced international experience in the relevant field of knowledge.

6.3 Requirements for organizing practices:

The educational program of the scientific and pedagogical magistracy includes two types of practices that are conducted in parallel with theoretical training or in a separate period:

1) pedagogical in the DB cycle - at the university;

2) research in the PD cycle - at the place of the dissertation.

Pedagogical practice is carried out with the aim of developing practical skills in teaching and learning methods. In this case, undergraduates are involved in conducting classes in a bachelor's degree at the discretion of the university.

The research practice of the undergraduate is carried out with the aim of acquainting with the latest theoretical, methodological and technological achievements of domestic and foreign science, modern methods of scientific research, processing and interpretation of experimental data.

7 ECTS Diploma Supplement

The application is developed according to the standards of the European Commission, Council of Europe and UNESCO / CEPES. This document is for academic recognition only and does not constitute official proof of education. Without a diploma of higher education is not valid. The purpose of completing the European application is to provide sufficient information about the diploma holder, the qualifications obtained by him, the level of this qualification, the content of the training program, the results, the functional purpose of the qualification, as well as information about the national education system. In the application model, which will be used for the transfer of estimates, the European system of transfer or credit transfer (ECTS) is used.

The European Diploma Supplement provides an opportunity to continue education in foreign universities, as well as to confirm national higher education for foreign employers. When traveling abroad for professional recognition will require additional legalization of the diploma of education. The European Diploma Supplement is completed in English upon individual request and is issued free of charge.

8 List of modules and learning outcomes

EP - Comprehensive information security
Qualification: Master of Engineering Science

Name module	Professional competence	Disciplines forming the module
Humanitarian module	Understand the philosophical issues of science, the main historical stages in the development of science, be able to critically assess and analyze scientific and philosophical problems, understand the specifics of engineering science, possess the skills of analytical thinking and philosophical reflection, be able to substantiate and defend one's position, possess the techniques of conducting discussion and dialogue, possess skills communicativeness and creativity in their professional activities. Be competent in matters of psychology and pedagogy.	History, philosophy of science, Pedagogy of higher education, Psychology of management
Module for	Be able to assess the security of network	Algorithms for

network security and cloud technologies and cryptographic protection of information	operating systems. Safely apply modern virtualization technologies.	cryptographic protection of information, Security tools for network operating systems, Security of virtualization systems and cloud technologies, Engineering and technical information security, Model-Driven Software Engineering, Steganographic methods of information protection
Module of scientific research, organization of information security system and ensuring information security	To be able to organize a database protection and security system and apply database protection technologies, know modern and promising directions for the development of cryptographic information protection and apply it in practice. To be able to organize comprehensive information protection and security. Be competent in cybercrime detection and computer forensics. Be able to use the means of recognizing and countering cyber attacks. Know and apply methods and tools for conducting information security audits. Know technical means and methods of technical protection of information, be competent in the organization, be component in the organization engineering and technical protection of information	Organization of protection and security of databases, Organization of information security systems, Numerical Methods in Engineering, Machine Learning & Deep Learning Cybercrime and computer forensics, Information security audit, Big Data and data analysis, Programming microcontrollers Risk management in cyber security, Security of systems of electronic business
Research module	Know technical means and methods of technical protection of information, be competent in the organization of engineering and technical protection of information. Be able to analyze big data, know methods and tools for analyzing big data.	Research work of the master student, Research practice.
Practice-oriented module	Presentation of current trends in the development of scientific knowledge. Knowledge of the methodology of scientific knowledge. The ability to formulate problems, tasks and methods of scientific research, to obtain new reliable facts based on observations, experiments, scientific	Pedagogical practice, research practice

	analysis of empirical data, to abstract scientific works, to compose analytical reviews of the accumulated information in world science and industrial activity, to generalize the results obtained in the context of previously accumulated in science knowledge, formulate conclusions and practical recommendations based on representative and original research results. Obtaining the competencies necessary for the implementation of scientific projects and research in the field of IT technologies.	
Final certification module	Obtaining the skills of independent research work and work in a research team. Ability to generate new ideas. Practice in the implementation of scientific projects and research in the professional field, in ways to ensure constant renewal of knowledge, expansion of professional skills and abilities. Ability to carry out information-analytical and information-bibliographic work with the involvement of information technology. Application of theoretical knowledge to develop and present your own conclusions when solving production problems in the IT sector. Ability to make decisions in difficult and non-standard situations in the field of organization and management of the enterprise.	Registration and defense of a master's thesis

9. Description of disciplines

Foreign language (professional)

Professional English for Project Managers
CODE – LNG202
CREDIT – 6 (0/0/3/3)
PREREQUISITES–Academic English, Business English, IELTS 5.0-5.5

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of the course is to develop students' knowledge of the English language for their ongoing academic research and improve their performance in the field of project management.

SHORT DESCRIPTION OF THE COURSE

The course is aimed at building vocabulary and grammar for effective communication in the field of project management and improving reading, writing, listening and speaking skills at the "Intermediate" level. Students are expected to develop their Business English vocabulary and learn grammar structures that are often used in a management context. The course consists of 6 modules. The 3rd module of the course ends with an intermediate test, and the 6th module is followed by a test at the end of the course. The course ends with a final exam. Master students also need to study independently (MIS). MIS is an independent work of undergraduates under the guidance of a teacher.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

Upon successful completion of the course, students are expected to be able to recognize the main idea and message as well as specific details while listening to monologues, dialogues and group discussions in the context of business and management; understand written and spoken English on topics related to management; write management texts (reports, letters, emails, minutes of meetings), following a generally accepted structure with a higher degree of grammatical accuracy and using business words and phrases, talk about various business situations using appropriate business vocabulary and grammatical structures - in pairs and groups discussions, meetings and negotiations.

History and philosophy of science

CODE – HUM201
CREDIT – 4 (1/0/1/2)
PREREQUISITES- HUM124

PURPOSE AND OBJECTIVES OF THE COURSE- to reveal the connection between philosophy and science, to highlight the philosophical problems of science and scientific knowledge, the main stages of the history of science, the leading concepts of the philosophy of science, modern problems of the development of scientific and technical reality

SHORT DESCRIPTION OF THE COURSE - the subject of the philosophy of science, the dynamics of science, the specificity of science, science and pre-science, antiquity and the formation of theoretical science, the main stages of the historical development of science, features of classical science, non-classical and post-non-classical science, philosophy of mathematics, physics, technology and technology, the specificity of engineering sciences, ethics science, social and moral responsibility of a scientist and engineer

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE - know and understand the philosophical issues of science, the main historical stages in the development of science, the leading concepts of the philosophy of science, be able to critically assess and analyze scientific and philosophical problems, understand the specifics of engineering science, possess the skills of analytical thinking and philosophical reflection, be able to substantiate and defend one's position, own methods of discussion and dialogue, possess the skills of communication and creativity in their professional activities

PSYCHOLOGY OF MANAGEMENT

CODE HUM204

CREDIT – 4 (1/0/1/2)

PURPOSE AND OBJECTIVES OF THE COURSE

The main goal of the course is aimed at studying the characteristics of the behavior of individuals and groups of people within organizations; determining psychological and social factors influencing the behavior of workers. Also, great attention will be paid to the issues of internal and external motivation of people.

The main goal of the course is to apply this knowledge to improve the effectiveness of the organization.

SHORT DESCRIPTION OF THE COURSE

The course is designed to provide balanced coverage of all the key elements that make up the discipline. It will briefly review the origins and development of the theory and practice of organizational behavior, followed by a review of the main roles, skills and functions of management with a focus on management effectiveness, illustrated with real-life examples and case studies.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

Upon completion of the course, students will know: the basics of individual and group behavior; basic theories of motivation; basic leadership theories; concepts of communication, management of conflicts and stress in the organization.

will be able to define the different roles of leaders in organizations; look at organizations from the point of view of managers; understand how effective management contributes to an effective organization.

HIGHER SCHOOL PEDAGOGY

CODE – HUM205

CREDIT – 4 (1/0/1/2)

PRE-REQUISIT

PURPOSE AND OBJECTIVES OF THE COURSE the course is aimed at studying the psychological and pedagogical essence of the educational process of higher education; the formation of ideas about the main trends in the development of higher education at the present stage, consideration of the methodological foundations of the learning process in higher education, as well as psychological mechanisms that affect the success of learning, interaction, management of subjects of the educational process. Development of psychological and pedagogical thinking of undergraduates.

SHORT DESCRIPTION OF THE COURSE. In the course of studying the course, undergraduates get acquainted with the didactics of higher education, the forms and methods of organizing education in higher education, the psychological factors of successful learning, the peculiarities of psychological influence, the mechanisms of educational influence, pedagogical technologies, characteristics of pedagogical communication, and mechanisms for managing the learning process. Analyze organizational conflicts and ways to resolve them, psychological destruction and deformation of the teacher's personality.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE – at the end of the course, the undergraduate must know the features of the modern system of higher professional education, the organization of pedagogical research, the characteristics of the subjects of the educational process, the didactic foundations of the organization of the learning process in higher education, pedagogical technologies, the patterns of pedagogical communication, the characteristics of educational influences on students, as well as the problems of pedagogical activity.

Organization of information security systems

CODE – SEC215
CREDIT – 6 (1/1/1/3)
PREREQUISITES– no.

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Organization of information security systems" (ISIB) is the formation of professional knowledge in the field of organization of information security systems at the facility.

The objectives of the discipline are: studying modern trends in international, domestic standards in the field of information security, building information security systems of an organization, developing an effective security policy and program depending on the objects of protection, the degree of its confidentiality, the use of modern methods, means and technologies for ensuring security.

SHORT DESCRIPTION OF THE COURSE

The curriculum program "Organization of information security systems" is aimed at familiarizing undergraduates with the basics of organization, construction, information security system, development of a program and security policy, defining objects of protection, forming a model of an intruder, organizing protection at the administrative, procedural levels of information security, conducting risk analysis and their assessment, to select methods, means and technologies of protection depending on the objects of protection, the degree of its confidentiality and the direction of business

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must have an idea of:

- about the basics of industrial relations and management principles;
- about modern research methods in the field of security;

As a result of mastering the discipline, the student must know:

- modern technologies in the field of information security, methods and means of computer technology and software;
- modern technologies in the field of information security;
- international standard for information security;
- legislative acts of the Republic of Kazakhstan in the field of information security;
- standards and specifications of information security and information protection harmonized in the Republic of Kazakhstan.

As a result of mastering the discipline, the student should be able to:

- create and apply modern technologies in the field of information security;
- apply modern information protection technologies in information security systems;
- manage information security of systems and networks.

Have skills:

- identifying threats and vulnerabilities in the organization's information security system;
- developing the organization's security policy and program;
- ensuring management and control at the administrative and procedural levels of the organization's information security;
- analysis and selection of information protection methods;
- ensuring and assessing the safety of the facility.

Organization of protection and security of databases

CODE – SEC214

CREDIT – 6 (2/0/1/3)

PREREQUISITES– Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Organization of protection and security of databases" (OZiBD) is the acquisition of professional competencies by students in the field of the organization of comprehensive protection and security of databases (DB).

The task of studying the discipline "Organization of protection and security of databases" is the assimilation of the basic principles of the organization of protection and security systems of database servers and their application.

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Organization of protection and security of databases" is aimed at studying technologies for ensuring the security of databases (DB). The course is devoted to the application of methods and tools for solving practical problems of protection and security of databases.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- organization of the database protection and safety system;
- database protection technologies and methods for designing secure databases;
- built-in mechanisms for ensuring database security in database servers;
- be able to:

- to apply in practice the technologies for ensuring the safety and protection of the database;

- to apply in practice the built-in mechanisms of database servers for the protection and security of the database;

have skills:

- designing secure databases in CASE tools;

using the SQL language to create, operate and ensure the protection and security of the database;

- the use of cryptographic built-in security tools.

Numerical Methods in Engineering

КОД - GEN200

CREDIT – 6 (1/1/1/3)

PRE-REQISIT – no

PURPOSE AND OBJECTIVES OF THE COURSE

This course aims at providing the necessary basic concepts of a few numerical methods and give procedures for solving numerically different kinds of problems occurring in engineering application.

SHORT DESCRIPTION OF THE COURSE

This course will cover a range of numerical analysis techniques related to solving systems of linear algebraic equations, nonlinear equations, polynomial approximation and interpolation, numerical integration and differentiation, ordinary and partial differential equations.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

The students will have a clear perception of the power of numerical techniques, ideas and would be able to demonstrate the applications of these techniques to engineering applications.

Machine Learning & Deep Learning

CODE – CSE746

CREDIT – 6 (2/0/1/3)

PRE-REQISIT – no

PURPOSE AND OBJECTIVES OF THE COURSE. The aim of the course is to master the basic theory and practice of machine learning methods based on widely used open access libraries. To teach how to apply machine learning models in practical problems of software development.

The main objectives of the course:

- Consider the main machine learning models and the tasks they solve
- Get an understanding and experience of neural networks
- Consider modern methods of data classification and clustering
- Exploring current research areas for Deep Learning Models

SHORT DESCRIPTION OF THE COURSE. The course focuses on deep learning models. As an area within machine learning, deep learning models illustrate quantitative-qualitative transition. New models and their properties require a separate study and practice of setting metaparameters of such models.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE. Upon completion of the course, students will:

Understand:

- Features of deep learning models
- Current Research Areas in AI

Know:

- Challenges and Applications of Deep Learning Models

Be able to:

- Use machine learning models.

Security of virtualization systems and cloud technologies

CODE – SEC244

CREDIT – 6 (2/1/0/3)

PREREQUISITES– no

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Security of virtualization systems and cloud technologies" (BSViOT) is to acquire students professional competencies in the field of virtualization and cloud technologies.

The task of studying the discipline "Security of virtualization systems and cloud technologies" is to master the basic principles of organizing the safe use of virtualization systems and cloud technologies.

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Security of virtualization systems and cloud technologies" is aimed at studying the technological foundations of cloud computing - the concepts of virtualization and virtualization systems, cloud technology services and ensuring their security and protection.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- technologies of virtualization of resources and platforms;
- virtualization systems from leading manufacturers;
- principles of building hypervisors and their vulnerability;
- threats and risks of virtualization systems;
- the main services of cloud technologies IaaS, PaaS and SaaS;
- common attacks on clouds;

be able to:

- install virtualization systems;
- work with cloud services;
- test virtual machines for vulnerability;
- create a virtual encrypted disk;

have skills:

- creating virtual machines;
- working with applications in a virtual machine;
- the use of cryptographic data protection in the clouds;
- using recommendations from the Cloud Security Alliance to ensure the security of cloud computing.

Cryptographic information protection algorithms

CODE – SEC201

CREDIT – 6 (2/0/1/3)

PREREQUISITES– Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of the discipline "Cryptographic information protection algorithms" is the formation of a system of professional knowledge about the rules governing the use of cryptographic transformations and algorithms for information protection, the development of skills for solving problems associated with the transformation and transmission of information.

The objectives of the discipline are: the study of cryptographic protocols used in the study and construction of modern algorithms, methods and models for transforming and protecting information; mastering the methods of analysis and implementation of cryptographic protocols; acquisition of skills in solving theoretical and practical problems.

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Cryptographic information protection algorithms" is aimed at acquainting undergraduates with cryptographic protocols, basic characteristics, properties that characterize the security of protocols; types of cryptographic protocols, attacks on the security of protocols, formal methods of analyzing security protocols; key distribution protocols; quantum cryptography and quantum key distribution protocols, secret sharing schemes, zero knowledge protocols, protocols for solving mathematical problems; bit binding protocol; game protocols of tossing a coin on the phone, playing poker on the phone; contract signing protocol.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- mathematical models of cryptographic protocols;
- modern technologies in the field of information security;
- formulation of scientific problems in the field of creation and research of rules governing the use of cryptographic transformations and algorithms;
- types of cryptographic protocols and information protection areas in which they are used;
- mathematical foundations of cryptographic protocols.

As a result of mastering the discipline, the student should be able to:

- - to solve mathematical problems arising in the creation of cryptographic protocols;
- to apply languages and programming methods to implement cryptographic algorithms;

- work with scientific publications devoted to the regulation of cryptographic transformations of information, and find practical application of the research results stated in the works;

- to perform the selection and assessment of cryptographic protocols when solving applied problems of cryptography

- create necessary modifications of the rules governing the use of cryptographic transformations and algorithms necessary for specific objects of information protection.

Have skills:

- analysis by mathematical methods of cryptographic protocols;

- skills in the implementation of basic algorithms that implement cryptographic protocols based on modern information technologies and network resources;

- possess knowledge of the mathematical apparatus of cryptography, necessary for research work.

- the skills of building cryptographic structures in which cryptographic protocols are present.

Steganographic methods of information protection

CODE – SEC 238
CREDIT – 6 (1/1/1/3)
PREREQUISITES – no

PURPOSE AND OBJECTIVES OF THE COURSE.

It is the development of the fundamental principles of steganography, which consist in ensuring the secret transmission and storage of confidential data by imperceptibly embedding them in other data transmitted through open channels.

SHORT DESCRIPTION OF THE COURSE

The content of the discipline covers a range of issues related to the protection of information through mathematical transformations using steganographic algorithms and copyright protection algorithms.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student should know:

- promising areas of development

- - classification of steganographic systems

- principles of construction of digital steganosystems, watermarks and steganosystems of data transmission.

- formats for presenting audio and graphic information in computer steganography systems

Be able to determine the steganographic stability of systems, apply software products in steganography and organize visual attacks on steganosystems.

Security Tools for Network Operating Systems

CODE – SEC 221
CREDIT – 6 (2/0/1/3)

PREREQUISITES– Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

Theoretical and practical training of students on the basics of organizing IP networks, routing, the peculiarities of the operation of IP protocols, types of network operating systems and ensuring their information security, as well as methods of protection against changes and control of the integrity of OS components (software). Course objectives: to form a general understanding of the security of network operating systems; familiarize with the organization of IP networks, with the internal organization of information storage in the OS; familiarize with the methods and means of ensuring the security of network operating systems; to gain practical skills in identifying threat foci and organizing protection in the OS.

SHORT DESCRIPTION OF THE COURSE

The course "Security Tools for Network Operating Systems" teaches the basics of organizing IP networks, the distribution of IP addresses, the scope and peculiarities of the operation of IP protocols, and types of network operating systems. Protection against alteration and control of software integrity. Methods and means of storing key information. Principles of multi-factor authentication. Identification and authentication technical devices. Password subsystems of identification and authentication. User identification and authentication using biometric devices. Encryption software and hardware. Ensuring security in Windows, Unix systems, familiarization with the internal organization of storage media. Intrusion detection systems. The main components of the firewall architecture. Modern requirements for firewalls.

Provides practical skills in intercepting and analyzing network traffic in order to identify threats. Viewing and analyzing the structure of file systems in order to organize protection against the spread of viruses within the system. Skills in software development (the development environment is chosen by the listener): 1) the exchange of short messages with the formation of IP packets between computers in the local network; 2) analyzing IP packets generated by the previous program and generating point DoS attack packets in order to provide a detailed presentation of network attack methods when setting up firewalls.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of studying the discipline, the student must know:

- organization of IP networks, structure of IP packets and IP protocols;
- internal organization of OS information carriers;
- methods and means of storing key information and encryption;
- types and principles of authentication;
- requirements for firewalls and intrusion detection systems;

have skills:

- interception and analysis of network traffic, as well as identification of vulnerabilities;
- analysis of the structure of file systems FAT32, NTFS, EXT4 and search, reading and changing information (in hexadecimal format) at the physical level;
- on the development of programs providing data exchange in a secure format between computers using various network protocols;

have the following competencies:

- use reference and informational materials to ensure the security of network operating systems;
- to carry out the choice of software and hardware security tools;

- develop algorithms and programs in low and high level languages;
- evaluate the security of network operating systems.

Model-Driven Software Engineering
CODE - CSE249
CREDIT – 6 (2/0/1/3)
PREREQUISITES – no

PURPOSE AND OBJECTIVES OF THE COURSE

SHORT DESCRIPTION OF THE COURSE

The purpose of the course is to study the principles and methods of software development of information systems. Principles of model-driven development. Models, specifications and their role in creating software systems. Model-oriented software engineering. General information about the Unified Modeling Language# General information about the unified modeling language and object constraint language. Domain-specific modeling languages.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

In the process of studying the discipline, undergraduates should:

- to know modern methods of design, analysis and application of information systems; to be able to apply various packages of instrumental software in the study of methods of development of information systems.

Have the skills of organizing the construction of models and algorithms for the functioning of information systems and managing the process of developing a software product in a team.

Engineering and technical information protection
CODE – SEC208
CREDIT – 6 (1/1/1/3)
PREREQUISITES– Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of teaching the discipline "Engineering and technical information security" is to familiarize undergraduates with the technical channels of information leakage, technical means and methods of unauthorized access to confidential information and protection of its security from leakage through various technical communication channels, as well as with the principles of construction and operation of technical means schemes acoustic reconnaissance and protection of information security from leakage through a radio channel, telephone lines, optical channel, etc.

The objectives of studying the discipline are to obtain knowledge on: technical channels of information leakage; technical means of unauthorized access to confidential information; technical means of wiretapping telephone communication channels and protecting information from leakage through these channels; methods and means of protecting information from leakage over a radio channel; technical means of protecting information from leakage through an optical communication channel; on filtering information signals, on noise suppression filters and on noise issues.

SHORT DESCRIPTION OF THE COURSE:

Secret, confidential and open information. Technical channels of information leakage. Technical means of acoustic reconnaissance. Technical means of unauthorized access to confidential information. Technical means of wiretapping telephone communication channels and protecting information from leakage through them. Technical means for searching and detecting embedded devices. Technical means of protecting information from leakage through an optical communication channel. Digital noise generator. White noise generators and their features .. Filtering information signals to suppress conducted noise. Technical channels of information leakage due to spurious electromagnetic radiation and interference (PEMIN).

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

At the end of the course "Engineering and technical information security" the master's student must **know:**

- types of confidential information, lists of confidential information;
- technical channels of information leakage and threats to information security as a result of unauthorized access;
- principles of construction and operation of circuits of electronic devices used in technical means of information protection;
- principles of operation and features of functioning of technical means of illegal removal and protection of information from leakage via radio, telephone and optical communication channels;
- questions of filtering information signals, interference filters and noise issues.

be able and have skills:

- to distinguish the types of protected information, to identify its sources and carriers;
- identify the main threats to information security and assess their degree;
- be able to use technical means of protecting acoustic information from leakage through various technical channels;
- possess the skills of working with the main hardware units of engineering and technical information protection;
- to apply the acquired knowledge in their further professional activities.

Information security audit

CODE – SEC204

CREDIT – 6 (2/1/0/3)

PREREQUISITES– Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Audit of information security" (AIB) is the acquisition of professional competencies in the field of audit of information security by students.

The objective of the discipline is the acquisition of theoretical and practical knowledge of the audit of information security (IS) of an enterprise by undergraduates.

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Audit of information security" is aimed at studying IS standards, organization and methods of auditing, their practical application.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- IS standards and IT security assessment criteria;
- types of audit and stages of audit;
- methods and tools for active audit;
- CVSS vulnerability assessment system;
- methods of data analysis during IS audit;

be able to:

- draw up an internal audit plan;
- to conduct an internal audit;
- use the CVSS vulnerability assessment system;
- use risk analysis tools;

have skills:

- conducting penetration testing;
- risk analysis.

Cybercrime and computer forensics

CODE – SEC240

CREDIT – 6 (2/1/0/3)

PREREQUISITES– Organization of information security systems**,** Средства безопасности сетевых ОС

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of the discipline "Cybercrime and computer forensics" is to acquire students professional competencies in the field of cybercrime and cybercrime investigation.

The task of studying the discipline "Cybercrime and computer forensics" is the assimilation of the principles of using systems and means of solving crimes related to computer information.

SHORT DESCRIPTION OF THE COURSE

Fundamentals of Forensics (computer forensics, cybercrime investigation) is an applied science about solving crimes related to computer information. The means of conducting digital evidence research and methods of searching, obtaining and securing evidence are being studied.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know: the basics of Forensics, questions and solutions of computer forensics; tools for researching digital evidence.

be able to:

- conduct investigations;
- explore digital evidence;
- apply modern methods and tools to detect cybercrimes.

Have skills:

- use of modern methods and means of investigation of cybercrimes;

- detection of cybercrimes;
- analysis of digital evidence.

Big Data and data analysis

CODE – SEC245

CREDIT – 6 (2/1/0/3)

PREREQUISITES– Organization of protection and security of databases, Security of virtualization systems and cloud technologies.

PURPOSE AND OBJECTIVES OF THE COURSE

The goal of the discipline "Big Data and Data Analysis" is to acquire professional competencies in the field of Big Data analysis by students.

The objective of the discipline is the acquisition of theoretical and practical knowledge on the analysis of big data by undergraduates, the use of special methods and analysis tools.

SHORT DESCRIPTION OF THE COURSE

The discipline is aimed at studying the creation, storage, management, transmission, retrieval, analysis of big data with an emphasis on the latest technologies, tools, architectures and systems, which are computing solutions with big data in high-performance networks. Real-world BigData applications and workflows in various fields (especially in science) are presented as use cases to illustrate the development, deployment, and implementation of a wide range of new BigData solutions.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- the latest technologies, tools, architecture and systems for big data analysis;
- solutions in the field of big data;
- methods of data collection, data storage and data analysis.

be able to:

- apply the latest technologies, tools and systems for big data analysis;
- to use in practice solutions in the field of big data;
- collect, store and analyze data.

have skills:

- conducting big data analysis
- application of methods and tools for working with big data.

Security of systems of electronic business

CODE – SEC206

CREDIT – 6 (2/1/0/3)

PREREQUISITES – Organization of information security systems, Organization of protection and safety of the database.

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline " Security of systems of electronic business" is the acquisition of professional competencies by students in the field of information security of economic systems (ES).

The task of the discipline " Security of systems of electronic business" is to master the basic principles of ensuring the safe operation of economic systems.

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Information security of economic systems" is aimed at studying theoretical and practical issues of ensuring information security of organizations of various forms of ownership.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student must know:

- RK standards for the protection of proprietary information;
- principles of organizing economic activity on the Internet;
- e-business models;
- threats to the security of economic systems;
- methods and means of information protection in ES;
- technologies for ensuring information security of ES;
- features of the protection of databases in the ES;
- organization of ES information security systems.

be able to:

- work with Web sites of different models of e-business;
- install and configure firewalls;
- install and configure intrusion detection systems;
- install and configure intrusion prevention systems;
- install and configure backup and data recovery systems;

have skills:

- intrusion detection;
- intrusion prevention;
- data backup and recovery.

Risk management in cyber security

CODE – SEC 245

CREDIT – 6 (2/0/1/3)

PREREQUISITES – Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Risk Management in Cybersecurity" (rmvkb) is to acquire professional competencies in the field of risk management in cybersecurity.

The objective of the discipline is to provide students with theoretical and practical knowledge on information security risk management

SHORT DESCRIPTION OF THE COURSE

The program of the training course "Risk Management in Cybersecurity" is aimed at studying risk management standards, risk assessment tools and their practical application.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student should know:

- basic concepts of risk in information security (IS);
- risk management standards;

- key issues of IS risk analysis and management;
- methods for assessing the company's information risks;
- quantitative and qualitative risk measures;
- tools for the automatic evaluation of risk (AOR);
- countermeasures that ensure the IB regime;

be able to:

- assess the risks;
- choose countermeasures to reduce the risk;
- choose countermeasures to avoid risk;
- choose countermeasures to change the nature of the risk;
- to use the tools of AOR;

have the skills:

- risk analysis;
- - risk assessments using EOR;
- risk taking.

Programming of microcontrollers

CODE – SEC 218

CREDIT – 6 (2/1/0/3)

PREREQUISITES – Organization of information security systems

PURPOSE AND OBJECTIVES OF THE COURSE

Study of the principles of building microprocessors and microcontrollers, programming of microcontrollers, as well as design, development and manufacture of electronic components of cryptographic systems using microcontrollers.

SHORT DESCRIPTION OF THE COURSE

Technical characteristics and software-available means of the microcontroller. Basic definitions, characteristics, scope and features of the operation of microprocessors. Varieties and architecture of microcontrollers. Design of cryptographic systems using microcontrollers. Modes of operation of the microcontrollers. Organization of the memory subsystem and interfaces. A system of interrupts and exceptions, as well as energy-saving modes. Types and characteristics of interfaces, direct memory access (DMA) coprocessors. Development trend of microcontrollers.

Design and development of circuit solutions based on CAD "Altium Designer". Programming the operation of individual blocks of microcontroller systems in the CooCox development environment.

Formation of skills programming in the C language of microcontrollers for solving various problems in cryptographic systems using the technical capabilities of microcontrollers.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

As a result of mastering the discipline, the student should know:

- format of data representation in microprocessor systems and their processing;
- electronic devices (photoelectronic devices, transistor, etc.);
- microchips (operational amplifiers, stabilizers, etc.) and their symbol (SMD components), purpose, standard sizes, characteristics.

Be able to:
- design and develop electrical circuits of electronic components using CAD;
- perform installation of electrical components of devices;
- apply measuring instruments in practice.

The educational program of the scientific and pedagogical magistracy includes two types of practices:

- pedagogical;
- research.

Pedagogical practice is carried out with the aim of developing practical skills and teaching methods. Pedagogical practice can be carried out during the period of theoretical training without interrupting the educational process. The research practice of the undergraduate is carried out with the aim of acquainting with the latest theoretical, methodological and technological achievements of domestic and foreign science, with modern methods of scientific research, processing and interpretation of experimental data.

Research work of a master student Research work in the scientific and pedagogical magistracy should:

- correspond to the main problematics of the specialty in which the master's thesis is being defended;
- be relevant, contain scientific novelty and practical significance;
- be based on modern theoretical, methodological and technological achievements of science and practice;
- carried out using modern methods of scientific research;
- contain research (methodological, practical) sections on the main protected provisions;
- be based on advanced international experience in the relevant field of knowledge.
- performed using advanced information technologies;
- contain experimental and research (methodological, practical) sections on the main protected provisions.

Master's project defense

CODE – ECA2013

CREDIT –12

The purpose of the master's thesis / project is:

demonstration of the level of scientific / research qualifications of a master student, the ability to independently conduct a scientific search, test the ability to solve specific scientific and practical problems, knowledge of the most general methods and techniques for their solution.

SHORT DESCRIPTION

Master's thesis / project is a final qualifying scientific work, which is a generalization of the results of independent research by a master's student of one of the topical problems of a particular specialty of the corresponding branch of science, which has internal unity and reflects the course and results of the development of the chosen topic.

Master's thesis / project is the result of the research / experimental research work of the master's student, carried out during the entire period of study of the master's student.

The defense of a master's thesis is the final stage of the master's preparation. Master's thesis / project must meet the following requirements:

- the work should conduct research or solve topical problems in the field of information security;

- work should be based on the definition of important scientific problems and their solution;
- decisions must be scientifically grounded and reliable, have internal unity;
- the thesis / project must be written individually;

Content