СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

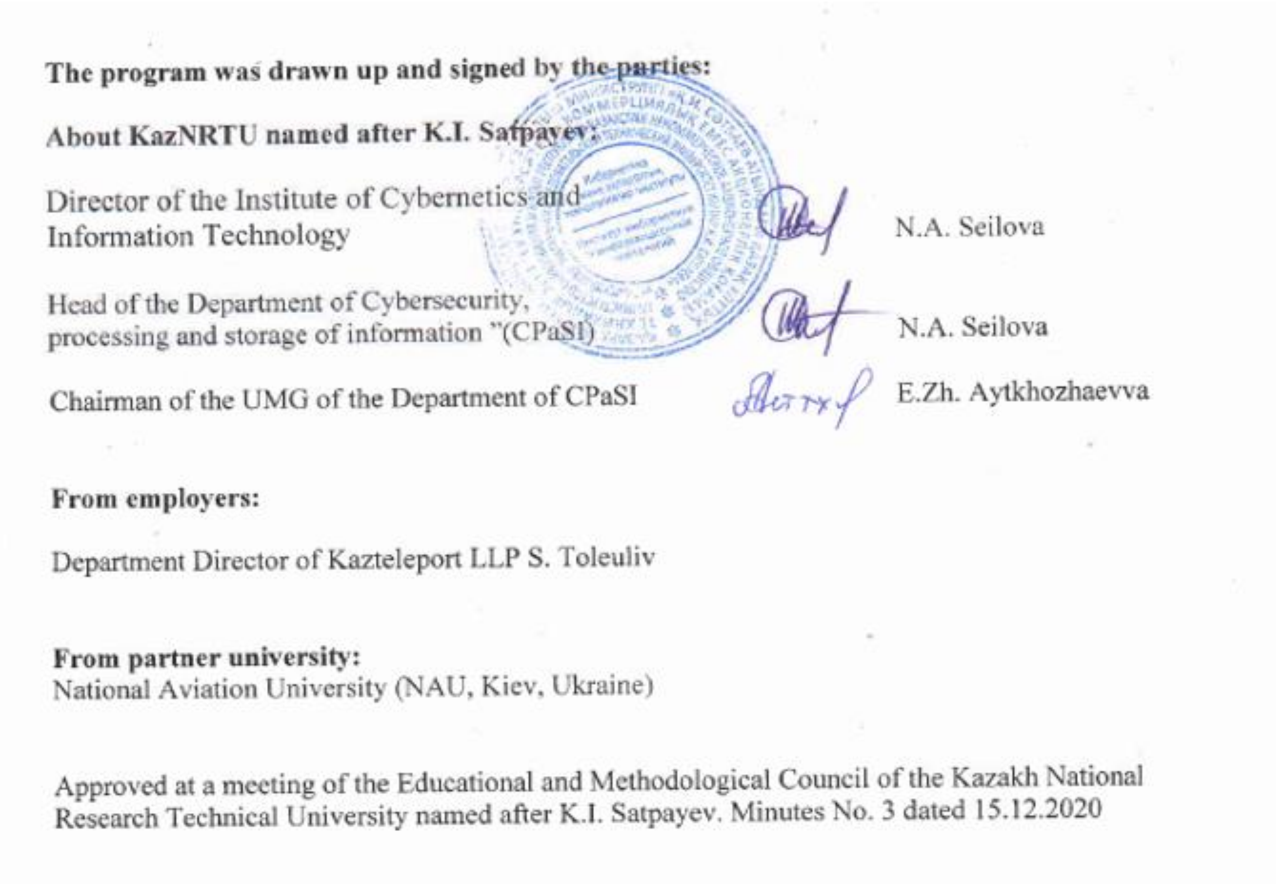
NPJSC «Kazakh National Research Technical University named after K.I. Satpaev»
Institute of Cybernetics and Information Technology
Department of "Cybersecurity, information processing and storage"

CURRICULUM PROGRAM

7M06110 - «COMPREHENSIVE INFORMATION SECURITY SUPPORT»
Master of Engineering and Technology (1,5 years)

1st 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.

Brief description of the program:

1 The purpose of the educational program:

The purpose of the educational program is to train undergraduates in the profile 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 masters is aimed at the protection and security of information, namely, the comprehensive provision of information security and engineering and technical protection of information.

Training of masters of the profile 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:

- 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 standard of education at all levels of education, order No. 604 dated 31.10.2018 and No. 180 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.
- ACM Recommendation for Curriculum in Computer Science (CC2005 Series).

The master of the educational program "Comprehensive 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 a 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 engineering and technology in the educational program "Comprehensive information security".

2 Types of employment

- - 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; planning an information security audit; maintenance of information security systems during its operation.

СӘТБАЕВ УНИВЕРСИТЕТІ 1934 SATBAYEV UNIVERSITY

EDUCATIONAL PROGRAM PASSPORT

1 Volume and content of the program

The term of study in the magistracy is determined by the volume of mastered academic credits. When mastering a set amount of academic credits and achieving the expected learning outcomes for a master’s degree, the master’s educational program is considered fully mastered.

Planning the content of education, the method of organizing and conducting the educational process is carried out by the university and the scientific organization independently on the basis of the credit technology of education.

The master's degree program implements educational programs of postgraduate education in management training with advanced professional training.

The content of the magistracy educational 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, professional internships;
3) experimental research work, including the implementation of a master's thesis;
4) intermediate and final certification.

Name: Comprehensive Information Security

The purpose of the educational program:

- Provide training for specialists for professional activities 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.
- Prepare production specialists for production activities related to the process of audit, monitoring, investigation of information security incidents, focused on 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:

1. 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 investigating 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 Entry Requirements

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

The procedure for admission of citizens to the magistracy is established in accordance with the “Model rules for admission to studies in educational organizations that implement educational programs of post-graduate 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 3 Requirements to complete the course and receive a diploma

Awarded degree / qualifications: A graduate of this educational program is assigned an academic degree of "Master of Engineering and Technology" in the educational program "Comprehensive information security.

A graduate who has mastered the master's degree program should have the following general professional competencies:

- the ability to independently acquire, comprehend, structure and use in professional activities new knowledge and skills, develop their innovative abilities;
- the ability to independently formulate research goals, establish the sequence of solving professional tasks;
- the ability to put into practice the knowledge of fundamental and applied sections of the disciplines that determine the direction (profile) of the graduate program;
- the ability to professionally choose and creatively use modern scientific and technical equipment to solve scientific and practical problems;
- the ability to critically analyze, represent, protect, discuss and disseminate the results of their professional activities;
- possession of skills for the preparation and execution of scientific and technical documentation, scientific reports, reviews, reports and articles;

- readiness to lead the team in their professional activities, tolerantly perceiving social, ethnic, confessional and cultural differences; - readiness for communication in oral and written forms in a foreign language for solving problems of professional activity.

A graduate who has mastered the master's program must have professional competencies corresponding to the types of professional activity to which the master's program is oriented:

- *production activities:*
- the ability to independently carry out production, field and laboratory and interpretation work in solving practical problems;
- ability to professional exploitation of modern field and laboratory equipment and devices in the field of mastered master programs;
- the ability to use modern methods of processing and interpreting complex information to solve production problems
- *project activity:*

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

- readiness to design complex research and production works 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 production work;
- - readiness for the practical use of regulatory documents in the planning and organization of scientific and production work in the field of information security.

When developing a master's program, all general cultural and general professional competencies, as well as professional competences related to the types of professional activities that the master's program is focused on, are included in the set of required mastering program results.

4 Working curriculum of the educational program

4.1. Duration: 1.5 years

Working curriculum of the educational program

Education program: **7M06110– «Comprehensive information security support»**

Duration of training: 1,5 years

Academic degree: Master of Engineering and Technology

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**						
	LNG 202	Foreign language (professional)	BD IC	6	3	0/0/3/3			Elective	PS CC	6	3		
	HUM204	Management psychology	BD IC	4	2	1/0/1/2			Elective	PS CC	6	3		
	MNG 274	Management	PS CC	6	3	2/0/1/3			Elective	PS CC	6	3		
		Elective	BD CC	6	3									
		Elective	PS CC	6	3				Elective	BD CC	4	2		
									Elective	PS CC	6	6		
									Elective	PS CC	6	3		
								AAP 221	Experimental and research work of the undergraduate, including the performance of the master's thesis	MSERW	4			
		In total		**28**					**In total**		**38**			
2	**3 semester**													
	AAP 246	Research practice		9										
	AAP 220	Experimental and research work of the undergraduate, including the performance of the master's thesis	MSERW	14										
	ECA 205	Registration and defense of the master's thesis	FA	12										

		(RaDMT)												
		In total		**35**										
									In all		**101**			

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

BD Choice component - 10 credits					
	Code	**Name of disciplines**	**Credits**	**Lec/lab/prac/IWS**	**Semester**
	CSE749	Methods and means of protection in Operating systems	6	1/1/1/3	1
	SEC 221	Means of security of network of operating systems	6	2/0/1/3	1
	SEC 238	Steganographic methods of information protection	4	1/0/1/2	2
	SEC 205	Safety and protection of cloud computing and telecommunications	4	1/1/0/2	2
		Total	**10**		
PS CC **Choice component - 36 credits**					
	CSE210	Models and methods of artificial int	6	2/1/0/3	1
	SEC246	Big Data and Data Analysis		2/1/0/3	1
	SEC222	Technologies of protection of wireless networks and mobile apps (applications)	6	2/1/0/3	2
	SEC215	Organization of information security systems	6	1/1/1/3	2
	SEC204	Information Security Audit	6	2/1/0/3	2
	SEC245	Risk management in cyber security	6	2/0/1/3	2
	SEC239	Analytical data warehouses and OLAP technologies	6	1/1/1/3	2
	SEC247	Intellectualized recognition and countermeasures for cyber attacks	6	1/1/1/3	2
	SEC218	Programming of microcontrollers	6	2/1/0/3	2
	CSE720	Cybercrime and computer forensics	6	2/1/0/3	2
		Total	**36**		

СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Modular educational program

Comprehensive information security support

(profile direction)

Academic degree: Master of Engineering and Technology Duration: 1.5 years

The cycle	**code**	**Name of disciplines**	**Semester**	**Acad. credits**	**lec.**	**lab.**	**prac**	**IWS**	**Type of contro**	**Chair**
Profile training module										
Basic disciplines (BD)										
University component										
BD	LNG202	Foreign language (professional)	1	6	0	0	3	3	Exam	EL
BD	MNG274	Management	1	6	2	0	1	3	Exam	SECPM
BD	HUM204	Management psychology	1	4	1	0	1	2	Exam	SECPM
Choice component (CC) (10 credits)										
Module for network security, security of cloud technologies and database systems										
BD	CSE749	Methods and means of protection in Operating systems	1	6	1	1	1	3	Exam	CIPaS
BD	SEC 221	Means of security of network of operating systems	1	6	2	0	1	3	Exam	CIPaS
BD	SEC 238	Steganographic methods of information protection	2	4	1	0	1	2	Exam	CIPaS
BD	SEC 205	Safety and protection of cloud computing and telecommunications	2	4	1	1	0	2	Exam	CIPaS
Major disciplines (MD)										
Choice component (CC) (36 credits)										
Module for data analysis, application of artificial intelligence in information security and ensuring the protection and security of information										
MD	CSE210	Models and methods of artificial int	1	6	2	1	0	3	Exam	CIPaS
MD	SEC246	Big Data and Data Analysis	1	6	2	1	0	3	Exam	CIPaS
MD	SEC222	Technologies of protection of wireless networks and mobile apps (applications)	2	6	2	1	0	3	Exam	CIPaS
MD	SEC215	Organization of information security systems	2	6	1	1	1	3	Exam	CIPaS
MD	SEC204	Information Security Audit	2	6	2	1	0	3	Exam	CIPaS
MD	SEC245	Risk management in cyber security	2	6	2	0	1	3	Exam	CIPaS
MD	SEC247	Intellectualized recognition and countermeasures for cyber attacks	2	6	1	1	1	3	Exam	CIPaS
MD	SEC239	Analytical data warehouses and OLAP technologies	2	6	1	1	1	3	Exam	CIPaS
MD	SEC240	Cybercrime and computer forensics	2	6	2	1	0	3	Exam	CIPaS
MD	SEC218	Programming of microcontrollers	2	6	2	1	0	3	Exam	CIPaS
Practice-oriented module										
MD	AAP246	Research practice	3	9					Report	

Research Module										
MSERW	AAP221	Experimental and research work of the undergraduate, including the performance of the master's thesis	2	4					Report	
MSERW	AAP220	Experimental and research work of the undergraduate, including the performance of the master's thesis	3	14					Report	
Module of final attestation (12 credits)										
FA	ECA205	Registration and defense of the master's thesis	3	12					Defense of dissertation	
Total				**101**						

5 Descriptors of the level and volume of knowledge, skills, abilities 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 degree) 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 field of digital diagnostics of equipment for mining, metallurgical and oil and gas production, based on advanced knowledge of this field, in the development and / or application of ideas in the context of the study;

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

3) to collect and interpret information for the formation of 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) training skills necessary for independent continuation of further education in the field of digital diagnostics of the equipment for mining, metallurgical and oil and gas production.

6 Competences to complete the training

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

1) 1) have an idea:

– - about professional competence in the field of information protection and security;

– - about the technology of virtualization of resources and platforms;

– - about database protection technologies;

– - about algorithms for cryptographic information protection;

– - about big data analysis.

2) to know:

- 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
- types and principles of authentication;
- requirements for firewalls and intrusion detection systems;
- database protection technologies and secure database design methods;
- organization of the database protection and safety system;
- methods and tools for active audit.

3) to be able to:

- to carry out information-analytical and information-bibliographic work with the involvement of modern information technologies;
- to think creatively and be creative in solving new problems and situations;
- be fluent in a foreign language at a professional level, allowing for scientific research and teaching of special disciplines in universities;
- apply algorithms for cryptographic information protection;
- apply IS standards and assess IT security;
- use virtualization systems from leading manufacturers;
- identify threats and risks of virtualization systems;
- 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) to have skills:

- 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 knowledge required for daily professional activities.

5) to be competent:

- 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, expansion of professional skills and abilities.

B - Basic knowledge, abilities and skills

B1 - knowledge and skills in the discipline Project management.

B2 - Know modern and promising trends in the development of cryptographic protection of information and apply it in practice.

B3 - Know the technologies of virtualization of resources and platforms, be able to apply virtualization systems from leading manufacturers.

P - Professional competencies:

P1 – to be competent in cybercrime and computer forensics, be able to identify threats and carry out intrusion prevention activities.

P2 - to be able to organize a database protection and security system and apply database protection technologies.

P3 – to know the issues of organizing information security systems and be able to carry out work in practice on integrated information security.

P4 – to be able to plan, design, install and maintain wireless security infrastructures.

P5 - to be competent in ensuring information security of economic systems.

P6 – to be able to analyze big data.

P7 – to know IS standards and IT security assessment criteria, be able to assess IS risks.

HS - Human, socio-ethical competences

HS1 - the ability to work in a team, have organizational skills, set priorities, quickly master new knowledge and skills, and apply them in practice;

HS2 – to be result-oriented, effectively plan and streamline your development;

HS3 - the ability to freely use English as a means of business communication, a source of new knowledge in the field of information security.

S - Special and managerial competencies:

S1 - independent management and control of the processes of labor and learning activities within the framework of the strategy, policy and goals of the organization, critical discussion of the problem, reasoning of conclusions and competent handling of information;

S2 - the ability to motivate to solve certain problems, the ability to take responsibility for the result of work performed at the level of a department or enterprise;

S3 - 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, to distribute and delegate authority, to form teams, and also to make decisions during the production process.

6.2 Requirements for the experimental research work of a master student in a specialized master's program:

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

2) is based on modern achievements of science, technology and production and contains specific practical recommendations, independent solutions to management problems;

3) it is performed using advanced information technologies;

4) contains experimental and research (methodological, practical) sections on the main protected provisions.

6.3 Requirements for organizing practices:

The educational program of the profile magistracy includes industrial practice in the PD cycle.

Industrial practice in the PD cycle is carried out with the aim of consolidating the theoretical knowledge gained in the learning process, acquiring practical skills, competencies and experience of professional activity in the taught educational program of the magistracy, as well as mastering advanced experience.

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 and Technology

Module name	Professional competence	Disciplines forming the module
Humanitarian module	master the techniques of discussion and dialogue, master the skills of communication and creativity in their professional activities. Be competent in management psychology and project management.	Project management (Psychology of management)
Module for network security, security of cloud technologies	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.	Methods and means of protection in Operating systems, Steganographic methods of information protection, Safety and protection of cloud computing and telecommunications
Module for data analysis, application of artificial intelligence in	Safely apply modern virtualization technologies. Know and apply the methods and tools for conducting information	Models and methods of artificial int, Information security risk

information security and ensuring the protection and security of information	security audits. Be competent in cybercrime detection and computer forensics. Be able to use the means of recognizing and countering cyberattacks. Be able to analyze big data, know methods and tools for analyzing big data.	management. Cybercrime and computer forensics, Big Data and data analysis Organization of information security systems, Technologies of protection of wireless networks and mobile apps (applications), Information Security Audit, Intellectualized recognition and countermeasures for cyber attacks, Programming of microcontrollers
Practice-oriented module	Getting professional skills. Ability to generate new ideas. Practice in performing research in a professional field, in ways to ensure a constant update of knowledge, expanding 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 field. Ability to make decisions in complex and non-standard situations in the field of organization and management of the enterprise..	Professional practice
Final certification module	Systematization and generalization of knowledge gained during master's studies for the successful completion of a comprehensive exam. Learning skill that allows you to continue learning largely independently and autonomously. Registration of the results of research and analytical work in the form of scientific articles, reports, analytical reports, dissertation. Ability to communicate their conclusions and the knowledge used to formulate them to specialists and non-	Registration and defense of a master's thesis

	specialists. Studying scientific and technical information, domestic and foreign experience in the field of IT technologies for its creative understanding and development of the correct solution to its scientific and technical or production problem.	

9. Description of disciplines

Foreign language (professional)
Professional English for Project Managers
CODE – LNG202
CREDIT– 6
PREREQUISITE –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.

BRIEF 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, SKILLS, SKILLS TO COMPLETE 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.

Management

CODE MNG274

CREDIT 6

PREREQUISITE: The discipline "Management" is based on the knowledge gained as a result of studying disciplines in undergraduate courses

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of teaching the discipline "Management" is to master the methodology of project management in various fields of activity, to foster a culture adequate to modern project management and information technology, to create conditions for the introduction of new information technologies in the implementation of projects. The course is based on international guidelines for project management (Project Management Body of Knowledge).

BRIEF DESCRIPTION OF THE COURSE

The content of the discipline is aimed at studying modern concepts, methods, project management tools in order to apply them in further practical activities of a specialist to solve problems of planning and executing projects.

KNOWLEDGE, SKILLS, SKILLS TO COMPLETE COURSE

To be able to:

- prepare documents for the initialization phase of the project, such as a feasibility study, project charter, etc.
- develop and analyze documents related to the planning of project activities, apply various methods of decision support;
- operatively control the execution of work and track the deadlines;
- select personnel, resolve contradictions between team members;
- to manage the risks arising from the implementation of projects.

Knowledge gained during the course:

- Modern standards in the area of project management and their characteristics;
- PMI approach to project management;
- Investment planning;
- Accounting for project risks;
- Methods for optimizing the use of available resources;
- Ways of resolving conflict situations;
- Analysis of actual indicators for timely adjustment of work progress

Skills:

- project management in accordance with modern project management requirements; - apply in the project management process using MS Project software

PSYCHOLOGY OF MANAGEMENT

CODE HUM204

CREDIT – 4

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.

Means of security of network of operating systems

CODE – SEC 221

CREDIT – 6

PREREQUISITES– no

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.

Methods and means of protection in Operating systems

CODE – CSE749

CREDIT – 6

PREREQUISITES– no

SHORT DESCRIPTION OF THE COURSE

The basic concepts and provisions of information security in operating systems. Security risks of information in information systems. Security risks of OS. Security requirements of OS. Analysis of security the modern operating systems. Built-in security features of Windows, Unix, Mac OS. Statistics of the methods which are the cornerstone of the attacks to the modern OS. Demarcation of access to OS. Identification and authentication of OS users. Demarcation of access to resources to OS Windows, Unix, Mac OS. Audit in OS. Systems of protection of the software.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

methods and means of storing key information and encryption;

- types and principles of authentication;
- 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.

Steganographic methods of information protection

CODE – SEC 238

CREDIT – 4

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 of virtualization systems and cloud technologies

CODE – SEC205

CREDIT– 4

PREREQUISITE – no.

PURPOSE AND OBJECTIVES OF THE COURSE

The purpose of the discipline "Security of virtualization systems and cloud technologies" 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.

BRIEF DESCRIPTION OF THE COURSE

Cloud computing, distributed data processing. Models of cloud deployment: public, private, hybrid clouds. Models of cloud technologies IaaS, PaaS, SaaS. The use of virtualization, virtualization technology, data centers, telecommunications networks. Features and characteristics of cloud computing. Security of cloud technologies, sources of threats in cloud computing. Standards in the field of cloud security. Means for securing cloud computing. Encryption, VPN-networks, authentication, user isolation.

KNOWLEDGE, SKILLS, SKILLS TO COMPLETE 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.

Models and methods of artificial int

CODE - CSE210

CREDIT– 6

PREREQUISITE – no.

BRIEF DESCRIPTION OF THE COURSE

The purpose of teaching discipline "Models and methods of artificial intelligence" is studying of the principles of creation of systems of artificial intelligence, studying of mathematical methods in models of representation of knowledge and technologies of artificial intelligence

KNOWLEDGE, SKILLS, SKILLS TO COMPLETE COURSE

As a result of studying of discipline students have to know the principles of creation of systems of artificial intelligence; the mathematical methods used in models of representation of knowledge and technologies of artificial intelligence.

Big Data and data analysis

CODE – SEC246

CREDIT– 6

PREREQUISITE – no

PURPOSE AND OBJECTIVES OF THE COURSE

The aim 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.

BRIEF 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 BigData applications and workflows in various fields (especially in the field of science) are presented as use cases to illustrate the development, deployment and implementation of a wide range of new BigData solutions.

KNOWLEDGE, SKILLS, SKILLS TO COMPLETE 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 technologies for wireless networks and mobile applications

CODE – SEC222

CREDIT-6

PREREQUISITE – no

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of this course is to plan, design, install and maintain security infrastructures for wireless networks and mobile applications. Particular attention is paid to countermeasures against fraudsters, as well as private entrepreneurs.

BRIEF DESCRIPTION OF THE COURSE

In this course, you will become familiar with the features, protocols, and configurations for implementing authentication, key distribution, integrity, confidentiality, and anonymity in wireless networks for mobile users. The course introduces the security techniques used in existing systems such as WPAN, WLAN, UMTS, IMS. Proposed solutions for new networking technologies such as various types of ad hoc networks. Digital forensics in wireless systems.

KNOWLEDGE, SKILLS, SKILLS TO COMPLETE COURSE

Knowledge at the end of the discipline:

- knowledge about technologies and methods of information protection for communication systems that provide services for mobile users by wireless access networks;

- knowledge and understanding of security mechanisms and protocols in wireless communication systems, such as current technologies WLAN IEEE 802.11, WAN 802.16, GSM / UMTS / LTE, Ad-hoc and sensor networks.
- knowledge of some models, design principles, mechanisms and solutions used in the security of a wireless network to obtain authentication and key transport protocols.

Skills:

- acquisition of practical and analytical skills in the assessment of information security technologies and methods for communication systems that provide services for mobile users with wireless access networks.
- practical skills in technologies for protecting wireless networks and mobile applications.

Organization of information security systems

CODE – SEC215

CREDIT– 6

PREREQUISITE – 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.

BRIEF DESCRIPTION OF THE COURSE

The curriculum program "Organization of information security systems" is aimed at familiarizing students with the basics of organization, construction, information security system, development of a security program and 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, SKILLS, SKILLS TO COMPLETE COURSE

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

- 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.

Information security audit

CODE – SEC204

CREDIT – 6

PREREQUISITES– no

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.

Risk management in cybersecurity

CODE – SEC 245
CREDIT–6
PREREQUISITE –no

PURPOSE AND OBJECTIVES OF THE COURSE

The aim of the discipline "Risk management in cybersecurity" (RMSB) is to acquire students of professional competencies in the field of risk management in cybersecurity.

The objective of the discipline is the acquisition of theoretical and practical knowledge of information security risk management by students.

BRIEF 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, SKILLS, SKILLS TO COMPLETE COURSE

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

- basic concepts of risk in information security (IS);
- risk management standards;
- key issues of analysis and management of information security risks;
- methods for assessing information risks of the company;
- quantitative and qualitative risk measures;
- means of automatic risk assessment (ARA);
- countermeasures to ensure IS mode;

to be able to:

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

to have skills:

- risk analysis;
- risk assessment using AOR;
- risk taking.

Analytical data warehouses and OLAP technologies

CODE – SEC239
CREDIT– 6
PREREQUISITE – no

PURPOSE AND OBJECTIVES OF THE COURSE

Study of the principles of data processing technologies.

BRIEF DESCRIPTION OF THE COURSE

Online analytical processing, or OLAP , is an approach to answering multi-dimensional analytical (MDA) queries swiftly in computing.[1] OLAP is part of the broader category of business intelligence, which also encompasses relational databases, report writing and data mining.[2] Typical applications of OLAP include business reporting for sales, marketing, management reporting, business process management (BPM),[3] budgeting and forecasting, financial reporting and similar areas, with new applications coming up, such as agriculture**.**

Intelligent means of recognizing and countering cyber attacks
CODE – SEC247
CREDIT – 6
PREREQUISITES – no

PURPOSE AND OBJECTIVES OF THE COURSE

Get acquainted with the principle of operation of intellectualized means of recognition and countering cyber attacks. Apply in practice methods and means of recognizing and countering cyber attacks.

SHORT DESCRIPTION OF THE COURSE

Risks and channels of information leakage, classification of violators. APT (Advanced Persistent Threat) attacks. Data leakage protection technologies. Systems for recognizing and countering cyberattacks. DLP systems classification, methods of confidential information recognition. Stages of DLP systems operation. Development of intellectualized means of recognizing and countering cyberattacks of systems. Analytical tools for incident investigation and analysis.

KNOWLEDGE, ABILITY, SKILLS TO COMPLETE THE COURSE

Know:

- about technologies and methods of information protection of intellectualized means of recognition and counteraction to cyber attacks
- on the security mechanisms of intellectualized means of recognizing and countering cyber attacks.
- on models, design principles, mechanisms and solutions used in intelligent means of recognizing and countering cyber attacks.

Skills:

- application of technologies and methods of information protection to recognize and counter cyber attacks
- application of security mechanisms of intellectualized means of recognition and counteraction to cyber attacks.
- application of models, principles of construction, mechanisms and solutions used in intellectualized means of recognizing and countering cyber attacks.

Programming of microcontrollers
CODE – SEC 218
CREDIT – 6
PREREQUISITES – no

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.

Cybercrime and computer forensics

CODE – SEC240

CREDIT– 6

PREREQUISITE – no

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 to master the principles of using systems and means of disclosing crimes related to computer information.

BRIEF 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, SKILLS, SKILLS TO COMPLETE 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

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.

BREIF 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