Institute of Technical Automation and Information Technologies Кафедра
"Cybersecurity, information processing and storage"

EDUCATIONAL PROGRAM
"7M06302 - Integrated information security"
(the cipher and the name of the educational program)

Code and classification of the field of education: 7M06 Information and communication technologies
Code and classification of training areas: 7M063 Information Security
Group of educational programs: M095 Information Security
NRK Level: 7
ORC Level: 7
Duration of study: 1,5 years
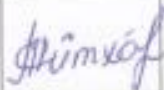Volume of credits: 90 credits

Almaty 2024

The educational program "7M06302 - Integrated information security"
was approved at a meeting of the Academic Council of KazNTU named
after K.I.Satpayev.
Protocol No. 13 of "28" __04__2022
Reviewed and recommended for approval at a meeting of the Educational and
Methodological Council of Kazntu named after K.I.Satpayev.
Протокол № 7 от "26" _04_2022 г.

The educational program "7M06302 - Integrated information security" was
developed by the academic committee in the direction "7M063 Information security"

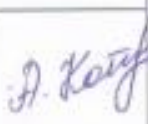| Full name	Academic degree/ academic title	Position	Workplace	Signature
Chairperson of Academic Committee:				
Viktor V. Pokusov		Chairman	Kazakhstan Information Security Association	
Teaching staff:				
Ryshan Zh. Satybaldieva	Candidate of technical Sciences	Head of the Department "Cybersecurity, Information Processing and Storage", Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 70-60	
Evgeniya Zh. Aitkhozhaeva	Candidate of technical Sciences, docent	Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Galim Z. Kaziev	Doctor of technical Sciences	Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Dulat N. Shukaev	Doctor of technical Sciences	Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Birzhan I. Zhumagaliev	Candidate of technical Sciences, docent	Associate Professor	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", internal phone: 73-61	
Employers:				
Amiret T. Konuspaev	Candidate of physical and Mathematical Sciences	President	Association of Innovative Companies of the Special Economic Zone "Park of Innovative Technologies"	
Orken Zh. Mamyrbayev	PhD, Associate Professor	Deputy General Director	RSE "Institute of Information and Computing Technologies"	
Students				
Atkeldy Ogan		1st year doctoral student	NCJS "Kazakh National Research Technical University named after K.I.Satpayev", mobile phone:+77076665721	

Oglavlanie

List of abbreviations and designations

EP – Educational program
BC – Basic competencies
PC – Professional competencies
LO – Learning outcomes
MOOC – Massive open online courses
NQF – National Qualifications Framework
IQF – Industry Qualifications Framework
IS – Information security
ICT – Information and communication technologies
IT – information Technology

1. Description of the educational program

The educational program 7M06302 "Comprehensive information security" is aimed at training master's students in a specialized field. The program includes basic and specialized disciplines with the achievement of relevant competencies, as well as various types of internships (production practice, experimental research and internship).

The professional activities of masters are aimed at the field of information protection and security, namely the comprehensive provision of information security and engineering and technical protection of information. Training of specialized masters in information security will be carried out according to the updated educational program 7M06302 "Comprehensive information security".

The programs of disciplines and modules of the educational program are interdisciplinary and multidisciplinary in nature, developed taking into account the relevant educational programs of the world's leading universities and the international classifier of professional activities in the field of information security. The educational program ensures the application of an individual approach to students, the transformation of professional competencies from professional standards and qualification standards into learning outcomes and ways to achieve them.

The educational program was developed based on an analysis of the labor functions of an information security administrator, information security auditor, and information security engineer, as stated in professional standards.

The main criterion for completing studies in master's programs is the mastery of all types of educational and professional activities of the master's student. Upon successful completion of the full course, the student is awarded a Master of Engineering and Technology degree in the educational program 7M06302 "Comprehensive information security."

A graduate can perform the following types of work:
- design and engineering; - production and technological;
- experimental research;
- organizational and managerial;
- operational.

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

2. The purpose and objectives of the educational program

Purpose of the OP: Training of 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 system.

OP tasks:

Training of highly qualified specialists who can solve the - planning of information security audit work following tasks:
- planning work on information security audit;
- organizational support for IS audit;

- carrying out an analysis of the compliance of design, operational and technical documentation on information security with the requirements in the field of ICT and information security support for the object of the information security audit;

- 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.

The master's degree in educational program 7M06302 "Comprehensive information security" is focused on independently determining the goals of professional activity and choosing adequate methods and means to achieve them, carrying out innovative activities to obtain new knowledge. In addition, it is focused on the organization, design, development, management and audit of applied information protection and security systems for all sectors of the economy, government organizations and other areas of activit.

3. Requirements for the evaluation of learning outcomes of the educational program

The educational program was developed in accordance with the State mandatory Standards of higher and Postgraduate Education, approved by the Order of the Minister of Science and Higher Education of the Republic of Kazakhstan dated July 20, 2022 No. 2 (registered in the Register of State Registration of Regulatory Legal Acts under No. 28916) and reflects the learning outcomes on the basis of which curricula are developed (working curricula, individual curricula of students) and working curricula in disciplines (syllabuses). Mastering disciplines of at least 10% of the total volume of credits of the educational program using MOOC on the official platform https://polytechonline.kz/cabinet/login/index.php/, as well as through the study of disciplines through the international educational platform Coursera https://www.coursera.org/.

Evaluation of learning outcomes is carried out according to the developed test tasks within the educational program in accordance with the requirements of the state mandatory standard of higher and postgraduate education.

When evaluating learning outcomes, uniform conditions and equal opportunities are created for students to demonstrate their knowledge, skills and abilities.

When conducting an interim certification in an online form, online proctoring is used.

4. Passport of the educational program

4.1. General information

№	Field name	Note
1	Code and classification of the field of education	7M06 Information and Communication Technologies
2	Code and classification of training areas	7M063 Information security
3	Group of educational programs	M095 Information security
4	Name of the educational program	7M06302 - Integrated information security
5	Brief description of the educational program	Professional activities of graduates include: education, government and departmental structures, economics and

		industry of the state, and healthcare. The objects of professional activity of graduates of master's programs in the educational program 7M06302 "Comprehensive information security" are: − government bodies; − information security departments and departments of departmental organizations; − information security departments, IT departments and departments of financial organizations; − information security departments, IT departments and departments of industrial enterprises; − departments and departments of information security of government organizations and commercial structures. The main functions of the professional activities of undergraduates are: conducting research in the field of information protection and security; audit, vulnerability analysis and incident investigation in information security systems; design, implementation, operation, administration, maintenance and testing of enterprise information security systems. Areas of professional activity are the following: − design, development, implementation and operation of information security systems; − analysis, testing and identification of system vulnerabilities; − information security audit
6	The purpose of the Educational program	Training of 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
7	Type of educational program	New EP
8	The level of the NRK	7
9	ORC Level	7
10	Distinctive features of the Educational program	No
11	List of competencies of the educational program:	A graduate of a specialized master's program must: 1) have an idea: − 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: − psychological methods and means of increasing the effectiveness and quality of training; − 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 constructing hypervisors and their vulnerabilities;
– organization of IP networks, structure of IP packets and IP protocols;
– internal organization of OS storage media;
– 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 security system;
– active audit methods and tools;
– engineering and technical protection of information.
3) be able to:
- critically analyze existing concepts, theories and approaches to the analysis of processes and phenomena;
- integrate knowledge gained within different disciplines to solve research problems in new unfamiliar conditions;
– through the integration of knowledge, make judgments and make decisions based on incomplete or limited information;
– carry out information-analytical and information bibliographic work using modern information technologies;
- think creatively and have a creative approach to solving new problems and situations;
– be fluent in a foreign language at a professional level, allowing you to conduct research;
– summarize the results of analytical work in the form of a dissertation, article, report, analytical note, etc.
– apply cryptographic information protection algorithms;
- apply information security standards and conduct IT security assessments;
- 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 methods for designing secure databases;
– organize a database protection and security system;
– apply active audit methods and tools;
- apply big data analysis tools.
4) have the skills:
– professional communication and intercultural communication;
– organization and protection of database security;
– conducting an information security audit;
– application of cryptographic information protection algorithms;
– identifying threats and countering them;
– working with Big Data;

		– expanding and deepening the knowledge necessary for everyday professional activities. 5) be competent: – in the organization of information security systems; – conducting an 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.
12	Learning outcomes of the educational program:	ON1. To be able to independently acquire, comprehend, structure and use new knowledge and skills in professional activities, develop their innovative abilities. Apply in practice the knowledge of fundamental and applied sections of the disciplines that determine the direction (profile) of the master's program ON2. Be competent in cybercrime detection and computer forensics. Be able to use the means of recognizing and counteracting cyber attacks. Know the technical means and methods of technical information protection, be competent in the organization of engineering and technical information protection. ON3. Be able to apply various decision support methods, quickly control the execution of work, resolve conflicts between team members, manage risks arising from the implementation of projects. Know modern standards in the field of project management and their characteristics. Proficiency in foreign languages. ON4. Be able to use regulatory documents in practice when planning and organizing research and production work in the field of information security. To know modern and perspective directions of development of cryptographic protection of information and apply it in practice. ON5. Know and apply resource and platform virtualization technologies and virtualization systems from leading manufacturers. Know the threats and risks of virtualization systems, the principles of building hypervisors and their vulnerabilities. ON6. Know the organization of IP networks, the structure of IP packets and IP protocols, the types and principles of authentication. Be able to assess the security of network operating systems ON7. Be able to organize the system of protection and security of the database. Apply database security technologies and secure database design methods. ON8. Be able to analyze big data, know the methods and tools for analyzing big data. Ability to formulate problems, tasks and methods of scientific research.
13	Form of training	full – time. online
14	Duration of training	1.5 years
15	Volume of loans	90 credits
16	Languages of instruction	Kazakh, Russian,
17	Academic degree awarded	Master of Technical Sciences
18	Developer(s) and authors:	Aitkhozhaeva E.Zh., Satybaldieva R.Zh.,

4.2. The relationship between the achievability of the formed learning outcomes according to the educational program and academic disciplines

№	Name of the discipline	Brief description of the discipline	Number of credits	Generated learning outcomes (codes)							
				ON1	ON2	ON3	ON4	ON5	ON6	ON7	ON8
1	Foreign language (professional)	The course is designed for undergraduates of technical specialties to improve and develop foreign language communication skills in professional and academic fields. The course introduces students to the general principles of professional and academic intercultural oral and written communication using modern pedagogical technologies. The course ends with a final exam. Undergraduates also need to study independently (MIS).	2			v					
2	Management	The purpose of the discipline is the formation of a scientific understanding of management as a form of professional activity; mastering the general theoretical provisions of the management of socio-economic systems by students; mastering the skills and abilities of practical solution of managerial problems; studying the world experience of management, as well as the peculiarities of Kazakhstani management, training in solving practical issues related to the management of various aspects of the activities of organizations	2			v					
3	Psychology of management (MOOC)	The course is aimed at mastering the tools for effective employee management, based on knowledge of the psychological mechanisms of the manager's activi ty. Discipline will help you master the skills of making decisions, creating a favorable psychological climate, motivating employees, setting goals, building a team and communicating with employees. At the end of the course, undergraduates will learn how to resolve managerial conflicts, create their own image, analyze situations in the field of managerial activity, as well as negotiate, be stress-resistant and effective leaders.	2			v					
Cycle of basic disciplines **Component of choice**											

4	Algorithms for cryptographic protection of information	The modern cryptography and tasks connected to information security problems. The formal determination of the cryptosystem. Classical cryptosystems. Main objectives of crypto-analysis. Stream encryption. Cryptosystems with public key. Applications of mathematical simulation in cryptography. Merits and demerits of different systems. Euler and Fermat's theorems. Key management. System without transmission of a key. Problem of prime factorization. Problem of the discrete logarithm. Crypto firmness problem. Systems of information security, diagram of the digital signature, authentication protocols and identifications.	4	v				v				
5	Security of Virtualization and Cloud Systems	In the process of studying the course, security issues of cloud technologies, sources of threats in cloud computing will be considered. Will be studied: cloud deployment models: public, private, hybrid clouds; cloud technology models; features and characteristics of cloud computing; information security standards in the field of cloud technologies and virtualization systems; means of ensuring the protection of cloud computing; encryption; VPN networks; authentication; user isolation.	5						v	v		
6	Cryptographic methods and means of information protection	Master's degree. Modern cryptography and tasks related to information security problems. Formal definition of a cryptosystem. classical cryptosystems. The main tasks of cryptanalysis. Stream encryption. Cryptosystems with a public key. Applications of mathematical modeling in cryptography. Advantages and disadvantages of various systems. Euler's and Fermat's theorems. Key management, Keyless system. The problem of decomposition into prime factors. Discrete logarithm problem. The problem of cryptographic strength. Information security systems, electronic signature schemes, authentication and identification protocols	4	v				v				
7	Scientific Python	The course studies the general principles of working with data: loading, receiving and processing unstructured data, obtaining data through the API, visualizing and	5						v	v		

		publishing data, filtering, transforming, analyzing and interpreting data using well-known models of classification, clustering, regression, etc. The range of tasks covers methods optimization, stochastic modeling, Gaussian modeling, partial differential equations, Navier-Stokes equation, heat equations											
Cycle of profile disciplines **University component**													
8	Organization of information security systems	The concept of information security systems. Information security systems standards. Select an object to organize the system. Threat analysis and security software development. Administrative and procedural levels of information security. Analysis and selection of information security methods. Provision and evaluation of objects	5	v		v							v
9	Production practice I	The production practice is aimed at strengthening knowledge and developing practical experience in the field of information security. The objectives of the practice include the participation of undergraduates in the organization of computer information protection, network technology, organization of computer systems and networks. The practice is aimed at the ability to independently carry out production, laboratory and interpretation work when solving practical problems.	5	v	v		v						
10	Production practice II	The production practice is aimed at strengthening knowledge and developing practical experience in the field of information security. The practice is aimed at the ability to use modern methods of processing and interpreting complex information to solve production problems.	4	v	v		v						
Cycle of profile disciplines **Component of choice**													
11	Data analysis and Data retrieval	The discipline is aimed to teach information retrieval and data mining techniques. It is about how to find relevant information and subsequently extract meaningful patterns out of it. While the basic theories and mathematical models of information retrieval and data mining are	5	v							v	v

		covered, the discipline is primarily focused on practical algorithms of textual document indexing, relevance ranking, web usage mining, text analytics, as well as their performance evaluations. Practical retrieval and data mining applications such as web search engines, personalisation and recommender systems, business intelligence, and fraud detection will also be covered.										
12	Information Security Audit	Audit of information security. Basic terms, definitions, concepts and principles in the field of information security audit. The main directions of the audit of information security. Types and objectives of the audit. The main stages of the security audit. A list of the initial data required to conduct a security audit. Assessment of the current state of the information security system. Assessment of the level of safety. Risk analysis, assessment of the level of security, development of security policies and other organizational and administrative documents for the protection of information. Effective programs to build an organization's security system	5		v		v				
13	Technical protection of information	Magistracy. Technical Protection (TP) of information. Actions for information security using passive and active technical means. Information ITZ technical means, classification. Physical security features of objects. Hardware of search and detection of channels of information leakage. Technical channels of leakage of acoustic information. Technical means of reception and information transfer. Mortgage devices of interception of the voice information. Telephone ear. Electronic stethoscopes. Laser microphones. Optical-electronic interception of audible tones by laser probing of windowpanes. The technical channel of information leakage by "high-frequency imposing". The parametric technical channels of information leakage.	5	v	v						
14	Intellectualized recognition and countermeasures for	Models, targets, tools of cyber attacks. Active protection as a method of countering advanced cyber threats. Effective counteraction. Components of active	5						v	v	

No.	Name	Description									
	cyber attacks	protection. Preventive network research. Analysis of anomalies. Advantages of active protection									
15	Information security of economic systems	Economic information as a commodity and a security object. Economic activity in the Internet. Types of security threats in economic information systems. Security policy. The main ways of unauthorized access to information. Methods and means of protection used in economic systems, their classification. Hardware security. Means of detecting information leakage channels. Firewalls. Intrusion detection systems. DLP system. Malicious programs. Systems of data backup and recovery. Cryptographic tools. Database protection. Cloud technology and data security	5				v			v	v
16	Cybercrime and computer forensics	The course is aimed at the study of digital evidence, methods of searching, obtaining and fixing such evidence, as well as the analysis and investigation of events in which computer information or a computer as a tool for committing a crime or other digital evidence appears. The course explores typical models of cybercriminals and their behavior, the main types of cyberattacks, as well as methods for responding, investigating and documenting cyber incidents.	5		v		v	v			
17	Organization of protection and safety of a database	Aspects and criteria of security, security policy. Data security threats. Database protection and security, data integrity and reliability. Methods and means of protection and data protection. Develop a secure database. CASE design tools. Database administration tools. Impressions as tools to improve data security. Effect of cursors on database security. Transaction management. stored procedures. triggers. Mandatory and discretionary access control to the DBMS. Role and reports. Monitoring and audit of DBMS. Cryptographic tools for database protection. Replication and data recovery. High training tools	5	v						v	
18	Risk management in cyber security	The program of the training course "Risk Management in Cybersecurity" is aimed at studying international and national standards for risk management in cybersecurity,	5				v				v

		methods for determining and managing risks, the practical application of standards and methods, studying specialized software systems for risk assessment										
19	Steganographic methods of information protection	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.	5	v			v					
20	Technologies of protection of wireless networks (applications)	Magistracy. Security technology for wireless networks and mobile applications. Unified solutions. Classification of applications for mobile devices. Methods for scanning and testing mobile applications. Integrated security system for wireless networks. Analysis of the security of mobile applications. Analysis of the security of mobile applications. Threats and security risks of wireless networks and mobile applications. Security protocols of wireless networks. WEP encryption mechanism. Passive and active network attacks. Authentication in wireless networks and mobile applications. Integrity and confidentiality of transmitted data. Deploying wireless virtual networks. Tunneling. IPSec protocol. Intrusion detection systems in wireless networks and mobile applications, their characteristics	5						v	v		
21	Big Data and Data Analysis	The purpose of the course is to form students' professional competence in the development and use of systems for processing and analyzing large amounts of data. The content of the discipline examines the methods of analysis and storage of large amounts of data, the stages of the life cycle of big data processing, the languages best suited for processing and analytics of big data, ways of organizing storage and access to big data	5	v							v	v
22	Machine Learning & Deep Learning	The course focuses on deep learning models. As a field within machine learning, deep learning models exemplify the quantitative-qualitative transition. New models and their properties require a separate study and practice of setting the metaparameters of such models. This course covers deep learning fundamentals, neural networks, convolutional networks, RNN, LSTM, Adam, Dropout,	5	v								v

#	Name	Description											
		BatchNorm, Xavier/He initializations											
23	OLAP and Data Warehousing	The purpose of mastering the discipline is to obtain in depth knowledge of data storage systems and data mining and data processing technologies. The content of the discipline includes questions on the types of data models, the concept and architecture of data warehouses, the implementation of procedures and examples of modern corporate systems using OLAP technology. Upon completion of the course, undergraduates will be able to design data ware houses and apply data processing technologies to solve research problems.	5									v	v
24	Security Internet of things	The purpose of mastering the course is to study the main areas of activity to ensure the security of the Internet of things, cyber-physical systems as part of critical information infrastructure facilities. As a result of mastering the discipline, undergraduates will learn to use the principles of a systematic approach; ways of forming requirements for the cybersecurity of the Internet of Things systems; the main provisions of the standards for the functional safety of process control systems ("Industrial Internet of things"); requirements of regulatory legal acts and standards for the development of information security threat models.	5		v								
	Experimental research work of a master's student												
25	Experimental research work of a master student, including an internship and the implementation of a master's projec	Systematization of theoretical knowledge, development of skills in setting problems on the research topic and solving them consistently. Research work includes assessing the objects of research, describing its problems, identifying a narrow area for research work, conducting an experiment, analyzing the results of the experimental part, preparing and defending a report on the EIR and summing up the results	18	v	v	v	v						

5. Curriculum of the educational program

KAZAKH NATIONAL RESEARCH TECHNICAL UNIVERSITY named after K.I.SATPAYEV

SATBAYEV UNIVERSITY

APPROVED
Chairman of the Management Board –
Rector of KazNRTU named after K.Satpayev
M.M. Begentayev
2024.

CURRICULUM
of Educational Program on enrollment for 2024-2025 academic year

Educational program 7M06302 - "Comprehensive information security "
Group of educational programs 7M095 - "Information security"

Form of study: full-time   Duration of study: 1,5 year   Academic degree: Master of Science

Discipline code	Name of disciplines	Cycle	Total amount in credits	Total hours	Classroom amount lec/lab/pr	SIS (including TSIS) in hours	Form of control	Allocation of face-to-face training based on courses and semesters		
								1 course		2 course
								1 semester	2 semester	3 semester
CYCLE OF BASIC DISCIPLINES (BD)										
M-1. Module of basic training (university component)										
LNG212	Foreign language (professional)	BD UC	2	60	0/0/2	30	E	2		
MNG726	Management	BD UC	2	60	1/0/1	30	E	2		
HUM211	Management Psychology	BD UC	2	60	1/0/1	30	E	2		
Component of choice										
SEC 201	Algorithms for cryptographic protection of information	BD, CCH	5	150	2/0/1	105	E		5	
SEC210	Cryptographic methods and means of information protection									
SEC404	Security of virtualization systems and cloud technologies	BD, CCH	4	120	2/0/1	90	E	4		
CSE403	Python for research activities				1/0/2					
CYCLE OF PROFILE DISCIPLINES (PD)										
M-2. Module of professional activity (university component)										
SEC215	Organization of information security systems	PD, UC	5	150	1/1/1	105	E	5		
SEC214	Organization of database protection and security	PD, UC	5	150	2/0/1	105	E		5	
SEC251	IT project and information risk management	PD, UC	4	120	2/0/1	90	E			4
component of choice										
SEC246	Big Data and data analysis	PD, CCH	5	150	2/1/0	105	E	5		
CSE746	Machine Learning & Deep Learning				2/0/1					
SEC248	Security Internet of things	PD, CCH	5	150	1/0/2	105	E	5		
SEC 222	Wireless network protection technologies									
SEC 204	Information security audit	PD, CCH	5	150	2/0/1	105	E	5		
SEC 245	Risk management in cybersecurity									
SEC234	OLAP and data warehouses	PD, CCH	5	150	1/1/1	105	E	5		
CSE258	Data analysis and data extraction									
CSE718	Engineering and technical protection of information	PD, CCH	5	150	1/0/2	105	E		5	
CSE238	Steganographic methods of information protection									
SEC240	Cybercrime and computer forensics	PD, CCH	5	150	2/1/0	105	E	5		
SEC247	Intelligent means of recognizing and countering cyber attacks				2/0/1					

M-3. Practice-oriented module										
AAP248	Production practice	PD, CCH	5						5	
M-4. Experimental research module										
AAP249	Experimental research work of a master's student, including internship and implementation of a master's project	ERWM UC	18							18
M-5. Module of final attestation										
ECA213	Registration and protection of the master's project (RaPMP)	FA	8							8
	Total based on UNIVERSITY:						40	20	30	
								60	30	

Number of credits for the entire period of study

Cycle code	Cycles of disciplines	Credits		
		university component (UC)	component of choice (CCH)	Total
BD	Cycle of basic disciplines	6	9	15
PD	Cycle of profile disciplines	19	30	49
	Total for theoretical training:	*0*	*25*	*39*	*64*
	ERWM			*18*
FA	Final attestation	8		8
	TOTAL:	8	25	39	90

Decision of the Academic Council of Kazntu named after K.Satpayev. Protocol № __12__ 22 ____04_____ 2024 y.

Decision of the Educational and Methodological Council of Kazntu named after K.Satpayev. Protocol № __6__ "_19__" ___04_____ 2024 y.

Decision of the Academic Council of the Institute AilT. Protocol №___8___ от "__29__" _____02_____ 2024 y.

Vice-Rector for Academic Affairs		Uskenbayeva R.K.
Acting Director of the AilT Institute		Kalpeyeva Zh.B
Department Head CIPaS		Satybaldiyeva R.Zh.
Representative of the Council from employers		Batyrgaliyev A.B.